ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/346602523

The Internet of Bodies: Opportunities, Risks, and Governance

Book · January 2020

DOI: 10.7249/RR3226

CITATIONS
26

READS
1,012

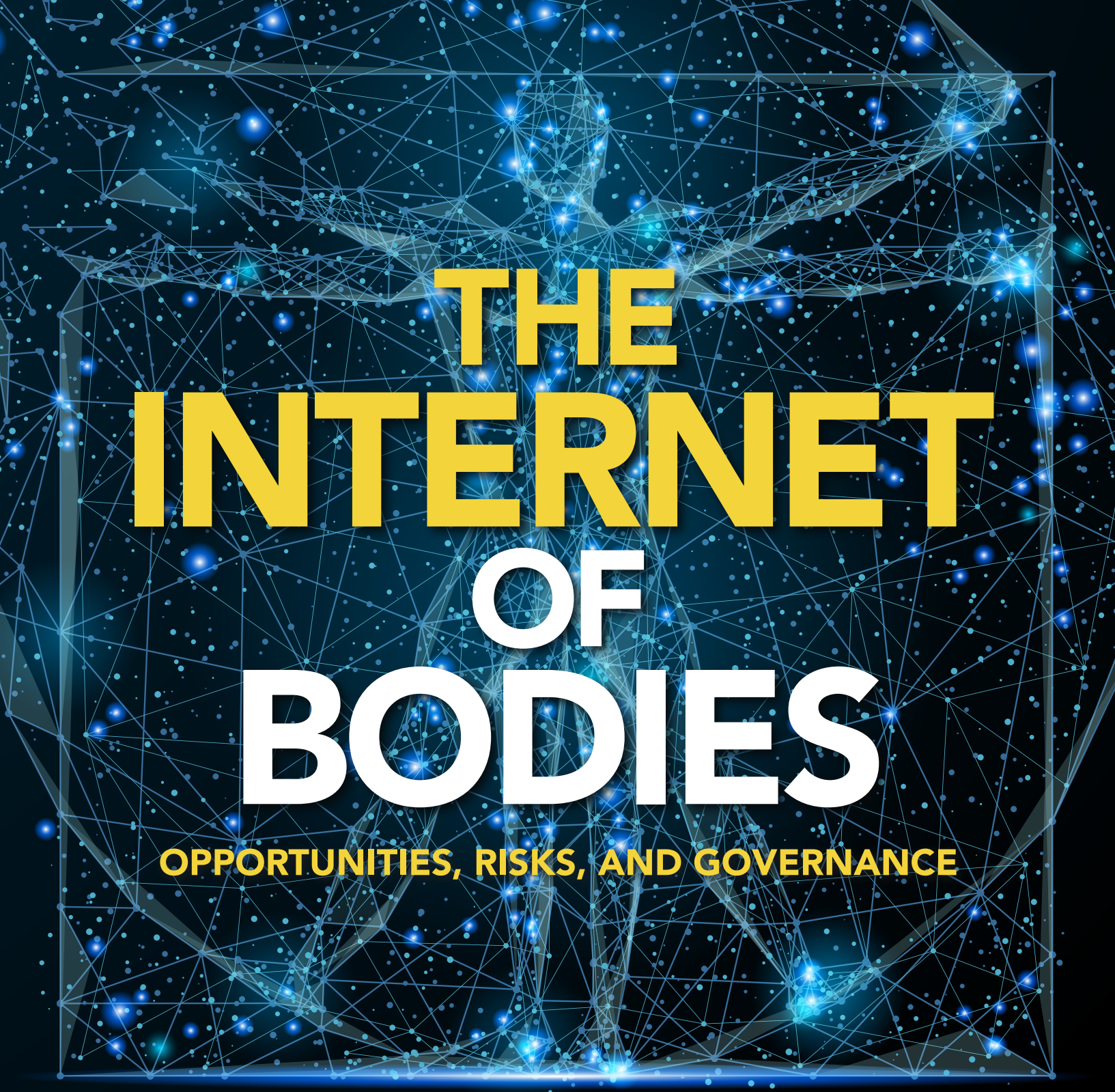
5 authors, including:

Benjamin Boudreaux
RAND Corporation
13 PUBLICATIONS **270** CITATIONS

SEE PROFILE

All content following this page was uploaded by Benjamin Boudreaux on 05 April 2024.

The user has requested enhancement of the downloaded file.



THE INTERNET OF BODIES

OPPORTUNITIES, RISKS, AND GOVERNANCE

MARY LEE | BENJAMIN BOUDREAUX | RITIKA CHATURVEDI
SASHA ROMANOSKY | BRYCE DOWNING

RAND CORPORATION

Cover Design: Peter Soriano
Cover Image: Adobe Stock/anttoniart.

Limited Print and Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited. Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please visit www.rand.org/pubs/permissions.html.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. **RAND**® is a registered trademark.

For more information on this publication, visit www.rand.org/t/RR3226

Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN: 978-1-9774-0522-7
© Copyright 2020 RAND Corporation

What Is the Internet of Bodies?

A wide variety of internet-connected "smart" devices now promise consumers and businesses improved performance, convenience, efficiency, and fun. Within this broader Internet of Things (IoT) lies a growing industry of devices that monitor the human body, collect health and other personal information, and transmit that data over the internet. We refer to these emerging technologies and the data they collect as the *Internet of Bodies* (IoB) (see, for example, Neal, 2014; Lee, 2018), a term first applied to law and policy in 2016 by law and engineering professor Andrea M. Matwyshyn (Atlantic Council, 2017; Matwyshyn, 2016; Matwyshyn, 2018; Matawyshyn, 2019).

IoB devices come in many forms. Some are already in wide use, such as wristwatch fitness monitors or pacemakers that transmit data about a patient's heart directly to a cardiologist. Other products that are under development or newly on the market may be less familiar, such as ingestible products that collect and send information on a person's gut, microchip implants, brain stimulation devices, and internet-connected toilets.

These devices have intimate access to the body and collect vast quantities of personal biometric data. IoB device makers promise to deliver substantial health and other benefits but also pose serious risks, including risks of hacking, privacy infringements, or malfunction. Some devices, such as a reliable artificial pancreas for diabetics, could revolutionize the treatment of disease, while others could merely inflate health-care costs with little positive effect on outcomes. Access to huge torrents of live-streaming biometric data might trigger breakthroughs in medical knowledge or behavioral understanding. It might increase health outcome disparities, where only people with financial means have access to any of these benefits. Or it might enable a surveillance state of unprecedented intrusion and consequence.

There is no universally accepted definition of the IoB.[1] For the purposes of this report, we refer to the IoB, or the IoB ecosystem, as *IoB devices* (defined next, with further explanation in the passages that follow) together with the software they contain and the data they collect.[2]

Abbreviations

AI	artificial intelligence
CCPA	California Consumer Privacy Act
CFIUS	Committee on Foreign Investment in the United States
CGM	continuous glucose monitor
CPAP	continuous positive airway pressure
EHR	electronic health record
EU	European Union
EULA	end user license agreement
FDA	U.S. Food and Drug Administration
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
H-ISAC	Health Information Sharing Analysis Center
HIPAA	Health Insurance Portability and Accountability Act
ICS-CERT	Industrial Control Systems Cyber Emergency Readiness Team
IoB	Internet of Bodies
IoT	Internet of Things
MDIC	Medical Device Innovation Consortium
NCD	noncommunicable disease
NFC	near-field communication
NIST	National Institute of Standards and Technology
NITRD	Networking and Information Technology Research and Development
PGHD	person-generated health data
RFID	radio frequency identification

An *IoB device* is defined as a device that

- contains software or computing capabilities
- can communicate with an internet-connected device or network

and satisfies one or both of the following:

- collects person-generated health or biometric data
- can alter the human body's function.

The software or computing capabilities in an IoB device may be as simple as a few lines of code used to configure a radio frequency identification (RFID) microchip implant, or as complex as a computer that processes artificial intelligence (AI) and machine learning algorithms. A connection to the internet through cellular or Wi-Fi networks is required but need not be a direct connection. For example, a device may be connected via Bluetooth to a smartphone or USB device that communicates with an internet-connected computer. *Person-generated health data* (PGHD) refers to health, clinical, or wellness data collected by technologies to be recorded or analyzed by the user or another person. *Biometric or behavioral data* refers to measurements of unique physical or behavioral properties about a person. Finally, *an alteration to the body's function* refers to an augmentation or modification of how the user's body performs, such as a change in cognitive enhancement and memory improvement provided by a brain-computer interface, or the ability to record whatever the user sees through an intraocular lens with a camera.

IoB devices generally, but not always, require a physical connection to the body (e.g., they are worn, ingested, implanted, or otherwise attached to or embedded in the body, temporarily or permanently). Many IoB devices are medical devices regulated by the U.S. Food and Drug Administration (FDA).[3] Figure 1 depicts examples of technologies in the IoB ecosystem that are either already available on the U.S. market or are under development.

Devices that are not connected to the internet, such as ordinary heart monitors or medical ID bracelets, are not included in the definition of IoB. Nor are implanted magnets (a niche consumer product used by those in the so-called bodyhacker community, described in the next section) that are not connected to smartphone applications (apps), because although they change the body's functionality by allowing the user to sense electromagnetic vibrations, the devices do not contain software. Trends in IoB technologies and additional examples are further discussed in the next section.

Some IoB devices may fall in and out of our definition at different times. For example, a Wi-Fi-connected smartphone on its own would not be part of the IoB; however, once a health app is installed that requires connection to the body to track user information, such as heart rate or number of steps taken, the phone would be considered IoB. Our definition is meant to capture rapidly evolving technologies that have the potential to bring about the various risks and benefits that are discussed in this report. We focused on analyzing existing and emerging IoB technologies that appear to have the potential to improve health and medical outcomes, efficiency, and human function or performance, but that could also endanger users' legal, ethical, and privacy rights or present personal or national security risks.

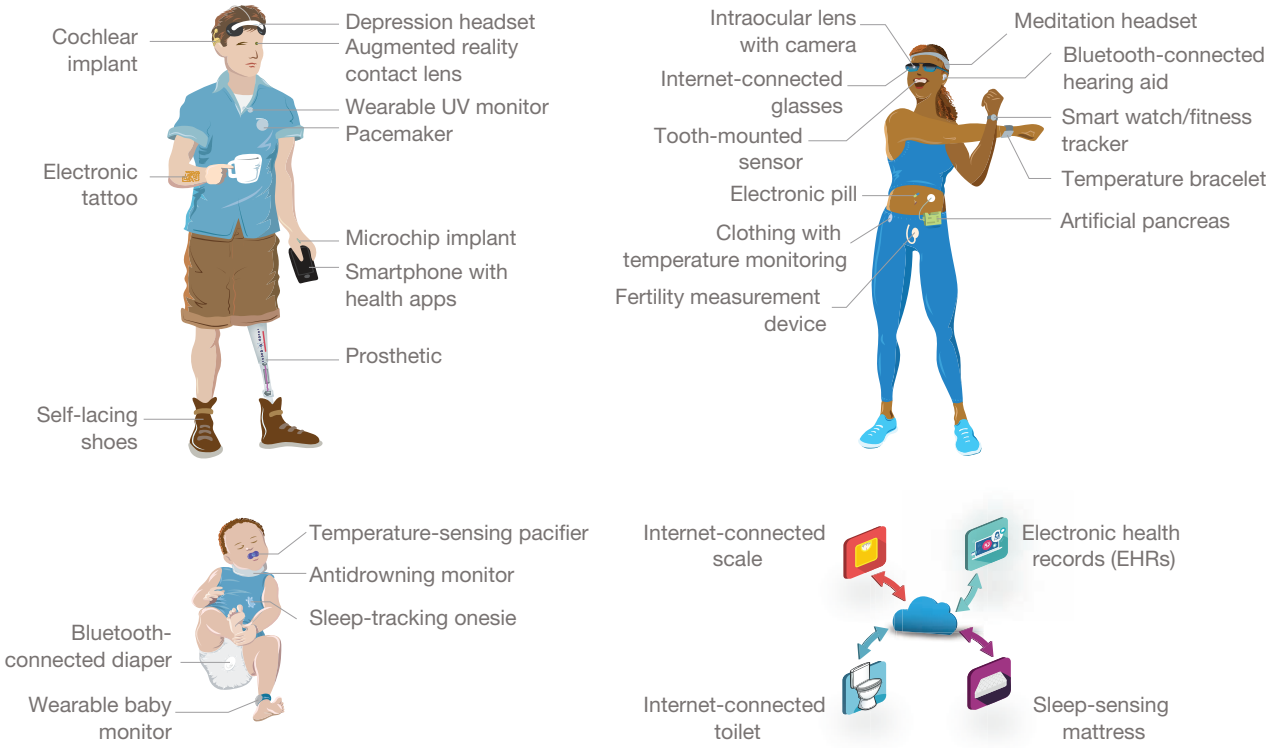
For this research, we conducted an extensive literature review and interviewed security experts, technology developers, and IoB advocates to understand anticipated risks and benefits. We had valuable discussions with experts at BDYHAX 2019, an annual convention for bodyhackers, in February 2019, and DEFCON 27, one of the world's largest hacker conferences, in August 2019. In this report, we discuss trends in the technology landscape and outline the benefits and risks to the user and other stakeholders. We present the current state of governance that applies to IoB devices and the data they collect and conclude by offering recommendations for improved regulation to best balance those risks and rewards.

An Emerging Landscape of Devices and Ideas

Internet of Things

IoB is closely related to the IoT,[4] which also has no universal definition; however, IoT devices do have

FIGURE 1
IoB Examples



several widely agreed-upon characteristics. First, IoT devices are connected to the internet either directly or through a local network. Second, they have at least one of the following functions: the ability to cause or sense some physical change, to directly get information from or provide information to humans, or to retrieve or store data. Finally, IoT devices must interact to provide some benefit to the user. For example, a lightbulb can be programmed to turn on at dusk without being connected to a network. It becomes part of the IoT only when it is connected to another IoT device, such as a smartphone, which then allows a user to turn on the light without being at home. Based on our definitions, any IoB device is an IoT device.

Our definition of the IoB includes technologies from what is often called *the health-care Internet of Things* (Healey, Pollard, and Woods, 2015), though not every health-care IoT device would be considered an IoB device. EHRs, robotic surgery systems, and devices used for medical treatment, such as smart ventilators, are all part of the IoB ecosystem because they collect users' information or alter the body's function. However, a hospital's "smart" refrigerator used for storing vaccines, which might be connected to a network and alert staff if stock runs low, is not an IoB device because it does not meet our definition.

Transhumanism, Bodyhacking, Biohacking, and More

The IoB is related to several movements outside of formal health care focused on integrating human bodies with technology. Next, we summarize some of these concepts,[5] though there is much overlap and interchangeability among them.

Transhumanism is a worldview and political movement advocating for the transcendence of humanity beyond current human capabilities. Transhumanists want to use technology, such as artificial organs and other techniques, to halt aging and achieve "radical life extension" (Vita-Moore, 2018). Transhumanists may also seek to resist disease, enhance their intelligence, or thwart fatigue through

diet, exercise, supplements, relaxation techniques, or nootropics (substances that may improve cognitive function).

Bodyhackers, biohackers, and cyborgs, who enjoy experimenting with body enhancement, often refer to themselves as *grinders*. They may or may not identify as transhumanists. These terms are often interchanged in common usage, but some do distinguish between them (Trammell, 2015). *Bodyhacking* generally refers to modifying the body to enhance one's physical or cognitive abilities. Some bodyhacking is purely aesthetic. Hackers have implanted horns in their heads and LED lights under their skin. Other hacks, such as implanting RFID microchips in one's hand, are meant to enhance function, allowing users to unlock doors, ride public transportation, store emergency contact information, or make purchases with the sweep of an arm (Baenen, 2017; Savage, 2018). One bodyhacker removed the RFID microchip from her car's key fob and had it implanted in her arm (Linder, 2019). A few bodyhackers have implanted a device that is a combined wireless router and hard drive that can be used as a node in a wireless mesh network (Oberhaus, 2019). Some bodyhacking is medical in nature, including 3D-printed prosthetics and do-it-yourself artificial pancreases. Still others use the term for any method of improving health, including bodybuilding, diet, or exercise.

Biohacking generally denotes techniques that modify the biological systems of humans or other living organisms. This ranges from bodybuilding and nootropics to developing cures for diseases via self-experimentation to human genetic manipulation through CRISPR-Cas9 techniques (Samuel, 2019; Griffin, 2018).

Cyborgs, or cybernetic organisms, are people who have used machines to enhance intelligence or the senses. Neil Harbisson, a colorblind man who can "hear" color through an antenna implanted in his head that plays a tune for different colors or wavelengths of light, is acknowledged as the first person to be legally recognized by a government as a cyborg, by being allowed to have his passport picture include his implant (Donahue, 2017).

Because IoB is a wide-ranging field that intersects with do-it-yourself body modification, consumer products, and medical care, understanding its benefits and risks is critical.

IoB Technologies

IoB technology has developed rapidly across a range of medical and consumer applications, with established medical companies and large technology firms increasingly joined by newer IoB start-ups. In this section, we present examples of IoB devices to demonstrate the range of technologies available or under development.

Medical Applications of IoB

Over the past decade, advances in medical technologies and data science have led to substantial growth in internet-enabled medical devices that promise better and more precise data to support patient care and improved health-care efficiency. These devices are used for a variety of diseases and conditions, including diabetes, seizures, and Parkinson's disease. Table 1 offers examples of internet-enabled medical devices that are implantable, and Table 2 shows some that are wearable or freestanding;[6] all of these IoB devices are already in use.

Consumer Applications of IoB

The consumer marketplace for IoB has grown rapidly, with a variety of new devices available or in development that are intended to improve everyday health and comfort and offer other conveniences. Table 3 identifies some examples.

Future Trends: More Connectivity, More Technologies

Advances in internet technology and connectivity will enable many more IoB and IoT devices to connect with each other and at much greater speeds. The fifth-generation mobile telecommunications network, 5G, can support around 1 million devices per square foot, compared with the previous 4G network, which can support around 4,000 devices in the same area (Zaino, 2019). Wi-Fi 6, the next generation of Wi-Fi

TABLE 1
Examples of Implantable Medical IoB Technologies

Type of IoB	Description
Artificial pancreas	The artificial pancreas system integrates continuous glucose monitor (CGM) and insulin pump technology with AI algorithms that automate insulin dosing based on inputs from the CGM (Boughton and Hovorka, 2019). Some diabetics have sought out obsolete insulin pumps to hack a security flaw that allows the pump to be connected with a CGM for a do-it-yourself artificial pancreas (Zhang, 2019).
Brain-computer interfaces (BCIs)	BCIs use electrodes that connect signals from the brain to a computer. They may be either implanted in the brain or noninvasive (wearable or attached to the skull). BCIs under development aim to read and type entire words directly from the brain, or control prosthetic limbs from the mind ("Imagining a New Interface," 2019; Etherington, 2019).
Brain electrical signals for Parkinson's	Deep brain stimulation—a surgical procedure that implants electrodes into part of the brain and connects them to a small electrical device implanted in the chest—was first approved for use in Parkinson's patients in the United States in 2002 (LeMoyne et al., 2019). In recent years, new advances like wireless control via a smartphone have made the technology more precise and personalized. Directional leads enable each patient's doctor to target therapy to specific areas of the brain (Okun, 2019). A smartphone app allows the patient to adjust settings to optimize daily activities.
Cochlear devices	A cochlear implant is an electronic device that partially restores hearing through a sound processor that fits behind the ear to capture sound signals. The processor transmits those signals to a receiver implanted under the skin that then stimulates the auditory nerve (Slager et al., 2019). In June 2017, the first implant with wireless connectivity to smartphones was approved by the FDA. This device enables patients to monitor hearing, adjust settings, view personalized hearing information, and locate missing sound processors from their smartphones.
Implantable cardiac pacing	Newer cardiac pacemakers, implantable cardioverter defibrillators, and ventricular assist devices can provide real-time and continuous information regarding a patient's cardiac fluctuations and enable remote device management to automate technical checks, such as battery status, lead impedance, and sensing or pacing thresholds (Stachel et al., 2013).
Implantable glucose monitors	CGMs measure blood glucose via a sensor placed under the skin, and the sensor transmits readings via Bluetooth to handheld receivers or a smartphone app. When glucose levels are too high or too low, patients receive notifications so they can adjust their insulin or boost their blood sugar levels (FDA, 2018b).
Implantable smart stents	Stents are traditionally used to reopen clogged blood vessels. Smart stents enable continuous monitoring of blood flow across the stent to alert providers to the possibility of new clogs (Chen et al., 2018).
Ingestible digital pills	In 2017, the FDA approved the first digital pill: aripiprazole tablets with an ingestible sensor embedded in the pill that records that the medication was taken. The system works by sending a message from the pill's sensor to a wearable patch that transmits the information to a mobile app so that patients can track the ingestion of the medication on their smartphones. Patients can also permit their caregivers and physician to access the information through a web-based portal (Trauth and Browning, 2018). Other ingestible digital pills are now available, including oral oncology drugs with a digital sensor to track adherence, dosing, and patient activity levels to develop better dosing regimens for chemotherapies.

technology, is also expected to improve connectivity by allowing more devices to transmit data and communicate with routers simultaneously (Kastrenakes, 2019). Satellite internet is being developed to enhance internet availability, including in remote areas, by putting thousands of satellites in low Earth orbit (Grush, 2019; Staedter, 2019). These advancements will enable consumer IoT technologies, such as smart home systems, to connect to IoB devices so that, for example, one's smart thermostat will be linked to her smart clothing and automatically can regulate the temperature in her home. Greater connectivity and the widespread packaging of IoB in smartphones and appliances—some of which might collect data unbeknownst to the user—will increase digital tracking of users across a range of behaviors.

Some devices under development—such as augmented-reality contact lenses or direct brain-writing—have the potential to significantly alter social life by enabling the recording and

TABLE 2
Examples of Wearable and Freestanding Medical IoB Technologies

Type of IoB	Description
EHRs	Digital repositories of a patient's medical history (including treatment history, genetic data, wearable device data, and other biometric information) that offer real-time, patient-centered information instantly to authorized users (Dinh-Le et al., 2019; Office of the National Coordinator for Health Information Technology, 2019).
Freestanding infusion pumps	Programmable infusion pumps and dose error-reduction systems are now commonly used in hospitals for intravenous medication delivery. These systems integrate medication databases with infusion pumps and allow for automation of alarm systems that alert providers when programming errors have occurred (Giuliano et al., 2018). Other systems connect the infusion pump to a patient's EHR, ending the need to program the pump.
Sensor-equipped hospital beds	Beds that contain sensors for body temperature, heartbeat, blood, oxygen, pressure, or other data that are sent to the central system of the hospital and enable health providers to instantaneously monitor patients' vitals (Bentley, 2018).
Wearable insulin pumps	Computerized devices that deliver insulin continuously in an attempt to mimic normal pancreatic insulin release. Programmable insulin administration can be integrated and augmented with CGM biosensors to provide real-time glycemic control ("How Insulin Pumps Work," 2019).
Wearable prosthetics	Prosthetics with electronic sensors to detect minute muscle movements to operate artificial limbs (Zlotolow and Kozin, 2012). Some are internet enabled and send feedback to manufacturers to improve technologies; some can track vital signs (Yang et al., 2017).
Wearable seizure monitors	Watches and other wearable devices that continuously monitor the user and alert family members and caregivers upon the onset of abnormal movement patterns similar to those caused by seizures, such as those caused by epilepsy (Wicklund, 2018).

replaying of all a person's interactions. Brain-reading and signaling neuro-devices are already on the market, but improved brain technology interfaces could succeed in improving cognition, memory, and control. Brain-reading and -writing could eventually be used to affect people's thoughts for benevolent or malicious ends (CPDP Conferences, 2018).

Militaries have shown an interest in IoB technologies to track the health and well-being of service members, enhance their cognitive and physical abilities, improve training, and enable enhanced warfighting capabilities—for example, with augmented-reality headsets or technology-infused exoskeletons that track warfighters' physical characteristics and possibly also their state of mind. Militaries have sought to develop neuro-devices that enable control over physical systems—for instance, decoding motor control signals from the brain to enable a pilot to fly a plane by using his or her thoughts (Emondi, undated). Such capabilities would enable faster battlefield decisions but might also introduce new risks to warfare, such as cyberattacks that directly affect a soldier's brain (Binnendijk, Marler, and Bartels, forthcoming).

IoB data might also spur medical, military, or other advances in unexpected ways. For example, in June 2019, it was reported that the U.S. Department of Defense has an infrared laser that can detect a person's unique cardiac signature (measurement of the heart's electrical rhythms) with over 95-percent accuracy from a distance of 200 meters, even through certain clothing (Doffman, 2019). If a database of EHRs with cardiac signatures were available, this laser could be used to monitor patient cardiac events in a hospital or to identify individual combatants in a war zone from afar with great accuracy (Hambling, 2019).

Evaluating the Health Benefits of the Internet of Bodies

By 2025, there will be more than 41 billion active IoT devices (International Data Corporation, 2019), generating 2.5 quintillion bytes of data daily (Marr 2018) on environment, transportation, geolocation, diet, exercise, biometrics, social interactions, and everyday human lives (Faiola and Holden, 2017; Piwek et al., 2016). This explosion in IoT devices will

TABLE 3
Examples of Consumer IoB Technologies

Type of IoB	Description
Attention monitors	Glasses that use brain activity and eye movements to track attention. They are designed to be used in schools or while driving and provide audio or haptic feedback when they sense the user is inattentive (Massachusetts Institute of Technology Media Lab, 2019).
Body-implanted sensors	Tissue-integrated biosensors under development may provide more precise and expansive bio-tracking than traditional wearables. These implanted sensors also may have additional functionality, such as a skin-grafted interface that enables the user to remotely control other devices (Khan, 2019). Tooth-mounted RFID sensors under development would track information on glucose, salt, and alcohol consumed by the user (Silver, 2018).
Clothing with sensors	Clothes that contain sensors to record body temperature and adapt to keep the wearer comfortable. There are also products for infants such as diapers that use a Bluetooth-connected app to detect and report bowel movements (Waters, 2019).
Female technology products	"FemTech" products are technologies intended to improve women's health. They include app-connected wearable devices that measure cervical mucus to track fertility, devices that assist women in strengthening their pelvic floor by encouraging and tracking kegel exercises, and sensors that measure contractions during labor (Jaramillo, 2019).
Freestanding consumer IoB	Internet-connected furniture and appliances that track and offer feedback on the user's well-being at home. These include toilets that monitor urine flow and sugar levels and report results through an app (Marr, 2019a); scales that are integrated with health apps to track and analyze fluctuations in body weight, body-mass index, and water weight (Ross, 2019); and beds equipped with sensors that connect to sleep-tracking apps to gather and record data on sleep patterns (Appleby, 2019).
Implantable microchips	RFID and near-field communication (NFC) microchips implanted into human bodies to store information, such as one's name and address (akin to the chips many pet owners put in their dogs). Some can be programmed to unlock doors or pay for goods, similar to smartphone payment systems (Gillan, 2019).
Mental and emotional sensors	Freestanding and wearable sensors can assess a user's mental and emotional states by analyzing facial expressions, voice intonations, and other audio and visual signals (Day, 2019; Clymo, 2018).
Vision and hearing aids	Vision and hearing aids to restore or augment perception and offer the possibility of recording video and audio. In 2017, the first U.S. patent of an implantable intraocular lens with video camera and wireless capabilities was issued (Strathspey Crown, 2017). "Hearables" are intended not only to assist with hearing loss but also to connect with virtual smartphone assistants to detect whether the user has fallen and other behavioral indicators (Tibken and Cheng, 2018).
Wearable health trackers	Bracelets, watches, rings, and smartphone apps that track steps, heart rate, sleep patterns, and other physical data, such as how much alcohol the wearer consumed (Turk, 2019). These devices operate by using advanced accelerometers and other sensors that can translate movement into digital measurements. Many devices also offer data analytics and displays to provide detailed information in accessible forms.
Wearable neuro-devices	Head-wearable neuro-devices record and monitor brain activity and stimulate the brain through electrical signals. Some are used to encourage the user to perform brain exercises. Others might send electrical signals to the brain to treat such conditions as chronic pain, depression, attention deficit disorder, and post-traumatic stress disorder (Coates McCall et al., 2019).

result in further popularity of IoB devices. IoB might offer subjective benefits, such as pleasure and convenience, but here we focus on evaluating whether, with increased understanding of patients' IoB information, medical providers can improve preventive health treatment, detect illness earlier, improve the accuracy of diagnosis, and treat disease more effectively in the formal health-care system.

In the sections following, we illustrate examples of medical and health IoB and the evidence regarding their benefits. IoB might enable wider access to health care by enabling inexpensive "distributed" or "democratized" health care or by decreasing the need for risky or costly medical intervention. Through greater health awareness, improved prevention, and more-effective intervention, IoB even has the potential to drive down health-care costs. But it is

important to note that many IoB technologies are too new to have developed a clinical evidence base on long-term outcomes. Rather, benefits to date are largely reported as improving day-to-day efficiencies for providers. It will be necessary to track the evidence base as IoB becomes more mainstream to understand the true effects of these devices on clinical outcomes.

Effects on Precision Medicine and Precision Public Health

Precision medicine and precision public health (Dolley, 2018) emerged to develop targeted health interventions to address unique needs of specific populations. Precision medicine is enabled by (1) a large body of subgroup-specific research suggesting that various health interventions are not broadly effective, and that stratified strategies may be necessary to improve equity; (2) the rise in voluminous, precise, continuous, and longitudinal data generated by IoB that offer unprecedented insight into the experiences of individuals; and (3) concurrent maturing of data science, which moves beyond coarse timescales and single-level effects to refined, multitimescale, multilevel, and intersectional analyses that better account for complex interactions between social determinants, behaviors, and health. These factors suggest that to the extent that IoB devices enable precision medicine, they may improve health outcomes for vulnerable or understudied populations.

IoB devices collect PGHD on virtually all aspects of lifestyles and behaviors, creating a treasure trove of information that can potentially advance understanding of long-term population health and precision public health interventions. PGHD collected by IoB devices allow for continuous monitoring of health status in real time, as well as collection of longitudinal data outside of—or in addition to—the intermittent monitoring that takes place in clinical settings (Lai et al., 2017). PGHD can inform correlations between individual behaviors, sociodemographics, and population-level factors, uncovering the complex relationships between acute and chronic stressors, diet, lifestyles, and overall health.

However, PGHD are only as powerful as the analyses developed to translate vast amounts of unstructured, disparate data into meaningful health insights and interventions. Machine learning, AI, and other data science techniques are used in addition to traditional statistics to recognize patterns in—and make predictions based on—large, empirical data sets (Lupton, 2013; Lupton, 2014). AI has been successfully incorporated into decision support in data-intensive specialties such as radiology, pathology, and ophthalmology (Yu and Kohane, 2019). As opposed to hypothesis-driven designs, data science allows for networked, multilevel correlations of several variables on health outcomes to develop complex risk predictions to aid in decisionmaking. It enables identification of digital indicators of health that can be used to monitor, influence, and maintain healthy behaviors in real time. For example, recent studies demonstrate that individual changes in frequency and intensity of physical activity can predict depression (Kumar et al., 2018), and that audio data harvested from people's mobile phone conversations can predict cognitive impairment (Stück et al., 2018). Such studies highlight a major opportunity to use IoB to create a synergistic feedback loop among researchers, health professionals, and consumers.

Racial and ethnic minorities, the socioeconomically disadvantaged, and discriminated-against populations continue to experience disproportionate adverse health outcomes (National Center for Health Statistics, 2016), despite decades of research correlating individual social determinants of health, such as demographics (e.g., age, gender, race), social or population characteristics (e.g., employment, neighborhood, housing), and associated behaviors (e.g., diet, exercise, drugs, alcohol) to variations in health outcomes (Marmot, 2005). Many public health approaches still use population averages to create "one-size-fits-all" interventions to increase the probability of achieving the best outcomes for most people (Glasgow, Kwan, and Matlock, 2018; Braveman et al., 2005), which might contribute to disproportionate adverse outcomes. IoB may help to combat this by further enabling precision medicine and precision public health.

Effects on Medical Care

Electronic Health Records

EHRs are promoted by the Office of the National Coordinator for Health Information Technology, part of the U.S. Department of Health and Human Services, to improve interoperability of health data. EHRs are digital repositories of a patient's medical history that offer real-time, patient-centered information instantly to authorized users. Though EHRs contain medical and treatment histories of patients, they are designed to go beyond standard clinical data collected in a provider's office and can include behaviors, living situations, and family history. Sophisticated EHRs can also contain genetic data and data from wearable devices and a variety of other sources.

EHRs facilitate evidence-based practice by integrating clinical guidelines and automation tools that supply providers with up-to-date recommendations for patient care (Allen-Graham et al., 2018). They have demonstrated improved productivity and resource management for hospitals and improved quality of care for patients (Entzeridou, Markopoulou, and Mollaki, 2018). For example, in a recent national survey, 88 percent of practices reported that their EHR produces clinical benefits for patients, and 75 percent reported that EHRs allow better care delivery. Reasons for clinical benefits included reduction in medication errors, improved patient safety, and improved personalized management of care (Jamoon et al., 2012).

As the IoB feeds richer, more disparate data into EHRs, there is reason to anticipate that it will help researchers and clinicians understand associations between environment, behaviors, health, and disease.

In-Patient Applications

IoB may allow better management of care and drug delivery in hospital settings. Interconnected machines sharing data (e.g., EHRs, clinical decision support, medication dispensation, ventilators, infusion pumps, hospital beds) may reduce errors and allow hospital staff to spend less time searching for patient records or drug information, tracking regulations, and inventorying supplies.

IoB may allow better management of care and drug delivery in hospital settings.

For example, programmable infusion pumps and dose error-reduction systems are now commonly used in hospitals to deliver intravenous medication in a precise and controlled manner. However, medication errors can occur as a result of user error in programming the pump. Newer infusion pumps allow for algorithmic automation of alarm systems that alert providers when programming errors have occurred by matching medications to dosing guidelines (Giuliano et al., 2018). Intravenous clinical integration (Downey et al., 2018) takes this one step further—a doctor enters a medication order in the EHR, and that order is transmitted directly to the infusion pump with the correct flow rates and dosages.

Sensor-equipped hospital beds take advantage of the large amounts of time patients spend in bed to track their vital signs and upload data into their EHR. Sensors can measure body temperature, heart rate, blood, oxygen, pressure, fluid intake and output, and other indicators. Providers can remotely review and monitor their patients and receive alert messages in case of any sudden change in the status of the patient (Downey et al., 2018). One systematic review found that continuous telemetry monitoring in hospitals via sensor-equipped beds and other systems improved patient outcomes and reduced time spent in critical care for patients as opposed to intermittent monitoring (Downey et al., 2018), suggesting that broad implementation of noninvasive monitoring may improve patient care.

Outpatient Treatment and Adherence Management

IoB treatment monitoring has been demonstrated to help patients adhere to their treatment schedules

while allowing doctors to track compliance with prescriptions. In 2017, the FDA approved the first digital pill: an aripiprazole tablet with an ingestible sensor embedded in the pill that records that the medication was taken. The product is approved for the treatment of schizophrenia, acute treatment of manic and mixed episodes associated with bipolar I disorder, and for use as an add-on treatment for depression in adults. Treatment adherence is critical for such disorders and is considered the single greatest factor that predicts relapse in patients (Papola, Gastaldon, and Ostuzzi, 2018). The system works by sending a message from the pill's sensor to a wearable patch. The patch transmits the information to a mobile application so that patients can track the ingestion of the medication on their smartphone. Patients can also permit their caregivers and physician to access the information through a web-based portal (Trauth and Browning, 2018).

Building on the success of that digital pill, an oral oncology drug with a digital sensor has also been developed to track adherence, dosing, and patient activity levels to improve dosing regimens for chemotherapies. Eventually, other such IoB-enabled treatment may give providers and caregivers new insights, allow remote care of patients, avoid hospital admissions, and improve response to therapy (Plowman, Peters-Strickland, and Savage, 2018).

Remote Monitoring of Chronic Conditions

The global phenomenon of an aging population (United Nations, 2015; Harper, 2006) has led to a substantial rise in incidence and prevalence of chronic, noncommunicable diseases (NCDs). Each year, nearly 41 million people die from NCDs, representing 71 percent of all global deaths. NCDs account for a disproportionate amount of health-care spending, as roughly the costliest 5 percent of patients account for roughly 50 percent of health-care costs (World Health Organization, 2018).

IoB is a promising approach for developing real-time remote health monitoring systems for NCD patients, most immediately diabetics and heart patients. Diabetes is endemic in most regions of the world. Recent developments in artificial pancreas technology, enabled by a variety of IoB devices, promise better glycemic control and remote monitoring of patients (Garg et al., 2017).

Research has demonstrated that monitoring of vital signs can help reduce rehospitalization by detecting anomalies early and allowing appropriate and timely interventions (Fanucci et al., 2013). The FDA has approved a wristwatch that tracks atrial fibrillation, alerting patients that they may need to see a physician (Apple, 2018). In addition, a study by the Center of Connected Health Policy found that remote monitoring of heart failure patients using IoB devices led to a 50-percent reduction in 30-day hospital readmission rate (Agboola et al., 2015). It was hypothesized that early detection and intervention through remote monitoring were the primary drivers of the reduction.

Saving Lives Through Alerts

IoB devices can gather vital data to provide medical alerts to doctors, patients, and caregivers. The FDA has approved a seizure-monitoring wristwatch that detects abnormal movement patterns. When this watch detects a repetitive shaking motion characteristic of certain seizures, it automatically sends text and phone call alerts to the patient's designated alert recipients. Clinical studies found the watch was able to correctly identify seizures in both adults and pediatric patients with an almost zero false-positive rate (Gutierrez et al., 2018).

IoB devices might also prove useful in guiding treatment for those who cannot speak or articulate their symptoms or thoughts, such as infants, stroke victims, or dementia patients, by alerting caregivers to significant changes in vital signs, for instance. Senior citizens may also benefit, for example, from sensors that can detect falls and call for emergency services. Researchers using such sensor technology found that it was even possible to predict the occurrence of a fall based on the user's walk patterns (Scott, 2018).

Disease Surveillance

Disease surveillance depends on data capture from a large number of individuals and hospitals spanning great geographic distances. IoB lends itself

particularly well to this purpose (Steele and Clarke, 2013) because sensors built into smartphones, wearable devices, and such public facilities as toilets or door handles could all be used to detect the presence of disease and track its spread throughout the population. This could enable intervention of such epidemics or pandemics as measles, Ebola, or the flu. Particularly noteworthy is the ability of IoB devices to determine the number of people who have come into contact with a disease but are not symptomatic, the so-called silent carriers who are critical to understanding disease incidence rates. IoB may be an effective solution to this critical denominator challenge (Purcell et al., 2016) by enabling tracking and analysis of silent carrier behavior.

Uncertainties in IoB Benefits: How the Promises Stack Up

While many IoB benefits have been realized in the formal medical sector, there remain uncertainties. Practical realities might prevent many IoB promises from being fulfilled, at least in the short term—for example, functional interoperability of EHRs has been a challenge (Sullivan, 2018), and the transition remains a work in progress. Medical providers have had a mixed reaction to other patient approaches to self-help, such as information-seeking through online health communities (Rupert et al., 2014). As with other DIY phenomena (e.g., the shift to automated teller machines), there may be long-term changes to economic activity (like shifts in consumption patterns enabled by impromptu spending). These changes may be premature to understand now but should be monitored by researchers as the IoB and other digitization evolve.

Evaluating the Risks of the Internet of Bodies

Computer software is inherently vulnerable to unintentional flaws or malicious abuse. Weaknesses in code can be exploited to steal or manipulate information collected by the device, disrupt its functioning, or otherwise cause it to behave in unexpected or unintended ways. IoB technologies suffer from the same attack vectors as other IoT and computing devices, but IoB devices have enhanced risks resulting from the confluence of several characteristics, including connection to the body, the kind and extent of the information collected, and how the information might be used. Table 4 summarizes IoB risks as a function of those who might obtain unauthorized, illegal, or unexpected access to the data or, through the device, to the body; anticipated vulnerabilities; and potential consequences. The IoB devices that are likely to pose the most dangerous consequences (right column of Table 4) are those that possess a large number of vulnerabilities (middle column of Table 4) that are exploitable by numerous actors (left column of Table 4).

TABLE 4
IoB Risks: Unexpected Access, Vulnerabilities, and Consequences

Who Might Gain Access?	What Are Potential Vulnerabilities?	What Are Possible Consequences?
• Criminals • Hackers (e.g., security researchers, hobbyists, malicious attackers) • Data brokers • Data fusion centers • Employers • Schools • Health-care providers • Insurance companies • Manufacturers • Criminal justice system • Governments	• Bodily dependence on device for health or functional purposes • Sensitive data collection, possession, or dissemination • Internet connectivity • Regulatory gaps • Hardware • Software	• Death or physical harm from malfunction or hacking • Global and national security challenges • Data breach • Passive collection or sharing of data without informed consent • Misuse or unexpected uses of data • Personal identification • Increased health disparities • Coercion to accept devices • Infringement on body autonomy

Global, National, and Personal Security Risks

In 2018, the fitness company Strava released detailed geolocation information of the exercise routes of its users. The Department of Defense had been encouraging health tracking devices in an effort to combat the obesity epidemic and conducted a pilot program that gave out fitness trackers to more than 2,000 soldiers in 2013 (Bushatz, 2013) and 20,000 soldiers in 2015 (Lilley, 2015). The maps Strava released were so detailed and comprehensive that they potentially exposed hidden military bases and camps of U.S. military and civilian personnel and the life patterns of service members (Hern, 2018). After the incident, the military modified its policy and no longer allows deployed service members to use such apps or devices (Copp, 2018).

This is but one example of how the explosion of innovation and adoption of IoB devices can present global and national security risks. Some of these risks can be anticipated. For example, doctors considered the possibility that Vice President Dick Cheney's pacemaker could be used to assassinate him. Cheney's original pacemaker was equipped with a wireless monitoring feature, which could potentially be hacked. In 2007, Cheney's device was replaced with one without wireless capability (Vaas, 2013). Other such IoB risks may not be so easily anticipated or addressed.

Connectivity of internet-connected devices is evolving in kind and quality and will be further enabled by communication technologies, such as 5G, next-generation Wi-Fi, and satellite internet. But communication systems are likely to be targeted by adversary nations and criminal hackers. New Wi-Fi protocols have already been shown to have security flaws (Goodin, 2019);[7] concerns have arisen about 5G (Ng, 2019), especially given the dominance of Chinese vendors in supplying hardware and services globally (Bryan-Low et al., 2019); and growing counterspace programs in China and Russia may threaten U.S. satellite-based systems (Defense Intelligence Agency, 2019). The increased connectivity in IoT and IoB devices may provide an increased attack surface that introduces more vulnerabilities through these networks.[8]

Foreign investment in and acquisition of American companies has long been a concern due to national security risks. The Committee on Foreign Investment in the United States (CFIUS) was established in 1975 to analyze transactions that might have implications for U.S. national interests (Jackson, 2019). CFIUS may recommend a suspension or prohibition of investment in an American company if it would allow a foreign entity to maintain or collect sensitive personal data of U.S. citizens. Therefore, outside investment in IoB companies will need to be examined closely. In 2016, the Chinese company Kunlun took control of Grindr, a popular gay dating app, but agreed to sell it in May 2019 following a CFIUS investigation (Wang, 2019). While CFIUS has not disclosed specific reasons for its opposition to Chinese ownership of Grindr databases, information on users' location, messages, and HIV status raises concerns of blackmail of U.S. officials or government contractors (Bauerle Danzman and Gertz, 2019).

Just as foreign possession of data on Americans' dating habits or HIV status could be used for nefarious purposes, U.S. consumers' biometric and health data might be exploited by adversaries who could compile data from numerous sources to build detailed profiles of their American targets. In May 2019, Chinese actors were indicted for identity theft, computer hacking, and conspiracy to commit fraud in the 2015 hack of Anthem, one of the largest health insurance companies in the United States (Groll, 2019; Larson, 2019). This breach compromised the data, some of which were sensitive medical data, of 80 million people (Whittaker, 2019), including an estimated one-half of all U.S. federal workers (ThreatConnect Research Team, 2015). Moreover, according to a 2019 report (Gryphon Scientific and Rhodium Group, 2019) prepared for the U.S.-China Economic and Security Review Commission, China already has direct access to large amounts of clinical and genetic data on U.S. residents via investments and partnerships with American health-care companies. China is also pursuing a long-term strategy to become a biotechnology leader and is rapidly advancing in the field through bidirectional investment with U.S. firms, research partnerships with American institutions, and recruitment of foreign- and Chinese-born scientists who have been trained in

the United States (Gryphon Scientific and Rhodium Group, 2019). This strategy may enable China to increase its foothold in accessing Americans' biometric data, at the level of both individual persons and subpopulations, whether by commercial means or espionage.

Increased IoB adoption might also increase global geopolitical risks, because surveillance states can use IoB data to enforce authoritarian regimes. For example, China is using DNA data in an attempt to surveil Uighurs (Wee, 2019). It has also been reported that China's social credit scoring system uses enormous amounts of aggregated data, including health records, on individuals to determine their trustworthiness and to incentivize desired behaviors (Marr, 2019b). Widespread IoB use might increase the risk of physical harm, espionage, and exploitation of data by adversaries.

Cybersecurity Risks

Cybersecurity risks are often grouped into three categories known as the *CIA triad*, for confidentiality, integrity, and availability (Center for Internet Security, undated). *Confidentiality* means that data are seen only by authorized entities; *integrity* means the data collected have not been tampered with; and *availability* ensures that the data are accessible when and where they are needed.

As of early 2019, the FDA was not aware of any injuries or deaths arising from the malicious attack or compromise of connected medical devices (FDA, 2019a).[9] However, vulnerabilities within these devices could accidentally cause physical damage or be exploited maliciously to inflict harm or death. For example, two well-known medical device vulnerabilities exist within implantable defibrillators and insulin pumps, caused by poorly implemented communication protocols between the device and the remote monitoring systems. In the first case, a vulnerability was found in the wireless communication software of a common implantable cardioverter defibrillator (FDA, 2019b). This vulnerability could enable an attacker to intercept the communication between the implanted device and the clinical programming devices or home monitoring machines in a way that could allow manipulation of data or insertion of false (malicious) commands to the implanted device. Similarly, in 2016, a security researcher discovered three vulnerabilities in the computer code for an insulin pump that could allow an attacker to inject malicious commands, causing serious harm (Beardsley, 2016).

In addition, there are concerns relating to the broader ecosystem in which IoB devices are used (Das, Zeadally, and Wazid, 2017). A physical device implanted or attached to the body will wirelessly connect with a monitoring device, such as one's smartphone, which will then relay information into a cloud service. The data are then accessible by an external party, such as the device maker or a medical practitioner. This constellation of hardware and software, physical and logical communication paths, and organizational boundaries introduces many layers of complexity that are each susceptible to failure, degradation, compromise, and attack.

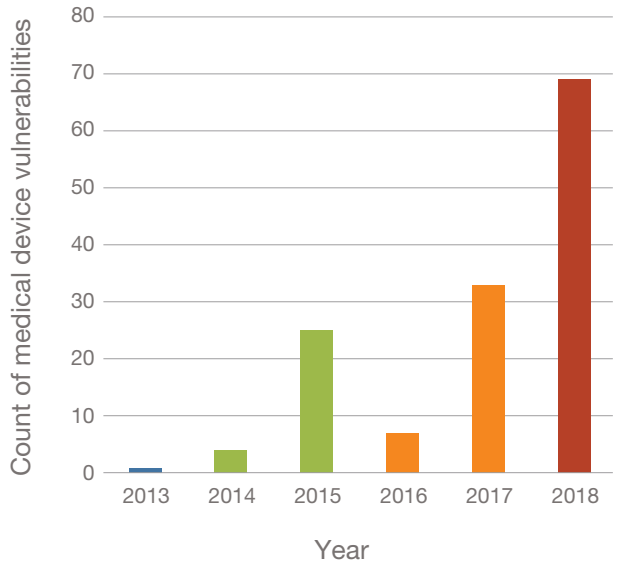
There have been efforts to catalogue the vulnerabilities discovered in medical devices. ICS-CERT (Industrial Control Systems Cyber Emergency Readiness Team), a division of the Department of Homeland Security, issues threat advisories for medical devices. Medcrypt, a health-care nonprofit organization, maintains an online document listing each of these advisories.[10] As of July 2019, it had documented 144 unique vulnerabilities discovered since 2013,[11] and the number of vulnerabilities is increasing,[12] as shown in Figure 2. We expect to see continual growth in IoB vulnerability reports merely because security researchers are starting to examine this burgeoning field.

Of the vulnerabilities found in these devices, a majority—65 percent—are flaws with user authentication and code defects. User authentication flaws might allow unauthorized users to access and associate data (e.g., compromise the confidentiality of the device). *Code defects* refers to software flaws that could allow a malicious user to breach the system's confidentiality, integrity, or availability. For example, a hacker might cause the device to share data with unauthorized users, manipulate the data so that the device behaves incorrectly, or simply make the device stop working.

IoB devices face several other unique security issues. Conventional cybersecurity recommendations

FIGURE 2

Medical Device Vulnerabilities, by Year



SOURCE: ICS-CERT threat advisories. ICS-CERT (Industrial Control Systems Cyber Emergency Readiness Team), a division of the Department of Homeland Security, issues threat advisories for medical devices.

include patching (e.g., installing new code to fix flawed code), applying mitigations (e.g., disabling the affected service or software component), and applying additional security controls on top of the vulnerable component to mask or otherwise block any incoming attack. However, in the cases of personal health devices that may be implanted inside a person's body, which require 24-hour availability or may not be serviceable in any practical way (for instance, if the patient lives in a remote area or is unable to visit a health facility), such mitigations may not be feasible or even possible.

In addition to the cybersecurity of the devices themselves, the repositories that store user data must also have sufficient security, software, and safety controls in place. If not, users might be in danger, as illustrated by the rapid adoption of EHRs. The 21st Century Cures Act of 2016 was meant to address difficulties with EHR adoption by improving health information system interoperability and patient access to data. In spite of this legislation, EHRs, which were in large part intended to alleviate medical errors, have been implicated in thousands of patient deaths, injuries, or near misses because of software flaws, user error, or other issues (Schulte and Fry, 2019a).

There may also be critical trade-offs between security and usability for IoB devices. Consider, for example, a connected insulin pump. Security best practices would suggest that access to the device be restricted to only those with proper authorization to release or modify the injections, something which is often done through usernames and passwords or via biometric login. However, a patient in insulin shock will likely not have the time or mental facilities to enter his or her credentials in the device. But ease of use may result in shortcuts to cybersecurity, and such shortcuts may threaten privacy.

Data and Privacy Risks

Data fuel the algorithms that serve up targeted advertisements, assess credit or other risk, and drive much of the internet economy. IoB devices collect and store highly personal data, arguably more intimate than any other type of user information, and so privacy and confidentiality risks abound. Information on users' whereabouts, bodily functions, what they see, hear, and even think could be recorded and stored.

There are many unresolved questions about who has authority to use data collected by IoB devices, and in what way. For example, there are questions about what law enforcement can do with IoB information, and whether such use is a violation of unreasonable search and seizure or self-incrimination protections guaranteed by the 4th and 5th Amendments to the U.S. Constitution. Medical information, such as pacemaker data, has already been used to charge people with crimes (Wootson, 2017). Concerns have been raised about how police are using data managed by state-owned and -operated data fusion centers, which aggregate and analyze personal data, including health data, from multiple public and private sources (Haskins, 2019). According to the analysis of one fusion center's user manual, information from various sources is "aggregated and synthesized in a way that gives law enforcement nearly omniscient knowledge over any suspect they decide to surveil" (Haskins, 2019). Other countries might have similar access to people's personal information and engage with the U.S. in reciprocity (mutual exchange) of

data (U.S. Immigration and Customs Enforcement, undated).

Data collection may threaten IoB users' privacy if safeguards are not in place to protect from misuse. The collection process itself, including what data are being collected, how often, whether informed consent was obtained (particularly in vulnerable populations such as minors or incarcerated persons), and whether the user can elect to stop the data collection or resale at any time, can pose an inherent risk to privacy.

IoB consumers appear to have accepted the need to provide their data to developers or others to use an IoB product. However, it is not clear that consumers have proceeded with complete knowledge regarding how their data are collected and may be used. An investigation into continuous positive airway pressure (CPAP) machines, used by those with sleep apnea, showed that patient data were being sent to insurance companies without users' knowledge to monitor their compliance (Allen, 2018a). If the patients did not use the CPAP machine for the required amount of time, the insurance company refused to cover the costs.

Information that reveals unhealthy lifestyle habits might have already resulted in higher health insurance premiums for some people (Allen, 2018b). An increase in IoB devices could escalate this trend of combining health data with other personal details, gathered by data brokers—companies that have no direct relationship with consumers but buy and sell their personal information—to increase premiums or limit access to care.

There is the question of inherent rights to which a user might be entitled. For example, should a user have the right to opt out, either of certain types of data collection or of storage? Should the U.S. implement a right to be forgotten for those who request deletion of their data?[13] Critics argue that the right to be forgotten could impinge on free speech (Bowcott, 2018), allow for an incomplete public record ("The Case Against a Right to Be Forgotten," 2018), or for history to be rewritten by authoritarian regimes (Swearingen, 2019). Another question is a posthumous right to privacy, i.e., once a person dies, should the data be expunged, or should it be accessible by next of kin?[14] This could be a particularly sensitive issue in the case of suicide, euthanasia, or fetal monitoring.

Furthermore, interpretation of IoB data, and algorithm outputs that rely on that data, may be biased or otherwise harmful to the user, particularly if there is little transparency into those processes (Osoba and Welser, 2017).

There are also concerns about data endurance—that is, results from a genetic testing kit or the use of a particular IoB medical device might identify someone as a carrier of a genetic disease that could be passed to his or her children, which could one day result in those children being denied certain insurance or other benefits (Klitzman, 2012).

Finally, there are as yet no legal norms about who owns the data generated by any given IoB device—the user, the manufacturer, the health-care provider? Data ownership has been a longstanding issue in health care (Meingast, Roosta, and Sastry, 2006). Business consulting firms are studying how IoT data can best be monetized (Deichmann et al., 2016; Russo and Albert, 2018). Policies that regulate the sale of user information to third-party data brokers, or that regulate how data brokers function, are nascent if they exist at all (MacMillan, 2019).

Ethical Considerations

Many of the risks previously discussed might be considered ethical in nature as they reflect values inherent to security and privacy. But we must also consider the potential harmful implications of IoB for other values important to Americans, such as equity and personal autonomy.

Inequitable Outcomes

One of the promised benefits of IoB technologies is decreased disparities in U.S. health-care outcomes by making preventive and diagnostic care less expensive and easier to access, but it is not clear that these technologies will decrease health-care costs or be readily accessible for the general population.

In general, advanced technologies in health care have contributed to an increase in overall costs (Callahan, 2008). Disparities due to access barriers to digital health and telehealth may be exacerbated

for those without reliable internet access (Gonzales, 2017). Many of those without insurance are not able to access advanced health-care technologies. Even for those insured, providers might not offer coverage for sophisticated IoB until and unless a cost-benefit analysis shows that such devices actually improve short- and long-term medical outcomes commensurate with their costs. This will require substantial evidence, and it will be important to know whether these benefits accrue across many population sectors (e.g., elderly patients who may be less technologically savvy, populations of low socioeconomic status, and so on).

Additionally, medical data are vulnerable to input bias, as typical users of IoB devices are a self-selecting group. Little is known about those who do not use IoB devices—whether by choice or because of cost or other barriers to access. Nonrepresentativeness of health data is a well-documented problem, because most clinical data are typically collected on middle- and upper-class, younger, white, male participants (Caplan and Friesen, 2017). Despite the 1993 Revitalization Act requiring clinical trials funded by the National Institutes of Health to include women and minorities, significant progress has not been made (Geller et al., 2018, 2011). Large-scale health data, though drawn from real-world populations, are not immune to input biases—EHRs and claims data involve patients that are actively engaged in health-care systems, resulting in samples that tend to be sicker or more disabled than the general population (Agniel, Kohane, and Weber, 2018; Verheij et al., 2018; Schneeweiss and Avorn, 2005). PGHD collected from consumers outside of the clinic may circumvent some of these biases but require other sampling considerations that are largely absent from early studies.

Freedom from IoB

As IoB becomes more ubiquitous, there may be increasing physical or psychological pressure on those who want to live their lives with minimal dependence on or interaction with these devices. Some IoB technologies can collect potentially sensitive information beyond the wearer or owner herself. For instance, augmented reality devices or "smart" hearing implants are designed to record video and audio. This might give rise to concern about privacy on the part of persons who are seen or heard by the devices but who have not consented to have their images or voices collected. One example of this phenomenon was the reaction to the Google Glass augmented reality system that generated public outcry—acutely illustrated in the "Stop the Cyborgs" movement (Farivar, 2013). The use of face recognition systems by law enforcement has led to criticism that the systems are biased, but also that they are being used to classify persons without their consent and with limited understanding of how the information will be used (Axon A.I. and Policing Technology Ethics Board, 2019). Similar criticisms apply to IoB with cameras and other tools that can be used to record or identify persons.

Some organizations have sought to use IoB to manage employees. While employee badges used to access the workplace would be considered IoB devices, there is a distinction between monitoring with passive feedback (e.g., the badge reader beeps and the building door unlocks to allow entrance) and monitoring with feedback that is networked (e.g., the device constantly keeps track of the user's whereabouts). Amazon has patented technologies for a wristband that can track employee behavior and that vibrates to nudge them to achieve greater productivity (Solon, 2018). Other technologies seek to identify when workers are sleepy or distracted (Derousseau, 2017). Researchers are creating wearables that claim to track an employee's workplace performance (e.g., amount of time spent at work, breaks from work, physical activity, and sleep levels) with about 80 percent accuracy (Holley, 2019). These capabilities might benefit employers and make them more data-driven and efficient (Knack et al., 2019), but they may alienate workers and harm retention if employees view them as intrusive and unnecessary.

Forcible adoption of IoB technology may be most likely to occur within the criminal justice system. Courts, prisons, or parole offices might pressure or require people to use IoB devices. Many jurisdictions use IoB ankle bracelets to prevent those awaiting trial from fleeing. Even if incarcerated persons do consent, they might be unaware of potential risks. One can envision IoB treatments akin to a digital aripiprazole

pill, used to treat psychiatric disorders, to take the place of traditional court-ordered psychiatric treatment. Other expanded requirements for those who have been arrested or convicted of crimes might be to use IoB to monitor their location, health, alcohol or drug use, or other indicators of perceived socially undesirable behavior.

Body Autonomy and Integrity

Another ethical consideration relates to users' rights over technologies that are integrated into their bodies. However, this right of users is in potential tension with attempts by technology developers to retain rights over software and devices. One example of this tension is the end-user license agreements (EULAs) that software developers employ to limit what a user can do to software following purchase. A EULA might restrict modifications to software or restrict its use to ensure intended performance or protect intellectual property. However, once a device is implanted in a person, the developer's continued proprietary control over the devices might become problematic (Matwyshyn, 2018; Matawyshyn, 2019; Atlantic Council, 2017; CPDP Conferences, 2018; Edinburgh Law School, 2018, at 26:28–28:08). For instance, what if a developer tries to force an agreement to a change of data-use policies related to a device that has already been (perhaps permanently) implanted? Some will argue that people have a fundamental moral right to bodily autonomy, and that right should enable them to have full control over their devices as an extension of their bodies.[15] Insofar as the users see the device as part of their body, they might reasonably believe that they have the right to resist developer-imposed changes. They might also insist on the ability to alter the device as they see fit. Already, there are examples of users "jailbreaking" or hacking IoB devices to improve their functionality (Brown, 2019; Hurley, 2014). However, developers have discouraged these modifications, arguing that they might negatively affect device functionality (Zhang, 2019).

Some varieties of IoB are largely unregulated—for instance, RFID bio-chips or health-tracking technology. But in the future, there might be a need to regulate the terms and conditions under which IoB technologies can be used and consider protections for certain vulnerable groups, especially to ensure that users have rights over technologies in their bodies.

Governance of IoB Devices and Information

As with most consumer products in the United States, governance of IoB devices is managed through a patchwork of direct and indirect state and federal agencies, nonprofit organizations, and consumer advocacy groups. For example, recall notices are sent both from the FDA (FDA, 2018c) and the Consumer Product Safety Commission (U.S. Consumer Product Safety Commission, 2018). The Federal Trade Commission (FTC) helps address IoT security (FTC, 2015) and health data breaches (FTC, 2010), and the National Institute of Standards and Technology (NIST) influences both civilian and governmental cybersecurity, with activity relating to IoT (NIST, 2019) and to cyber physical systems (NIST Cyber Physical Systems Public Working Group, 2016). In this report, we do not explore each organization in depth but provide a broad overview of the main governance influences related to the security and privacy of IoB devices. More specifically, we distinguish between regulations that apply to the IoB device itself and regulations that apply to the information collected, stored, or transmitted by the device. Despite the efforts to govern IoB, many of these devices and the information they collect evade regulatory scrutiny.

Governance of IoB Devices

The primary entities responsible for governance of IoB *devices* (we address *information* collected by IoB devices in the following section) are the FDA and the U.S. Department of Commerce.[16]

FDA Efforts

The FDA, a part of the U.S. Department of Health and Human Services, is responsible for the safety of medical devices. In hopes of fostering innovation in digital health, the FDA developed a Digital Health

Innovation Action Plan. However, the 21st Century Cures Act excludes the agency from having jurisdiction over EHRs. Former FDA Chief Scott Gottlieb has called on Congress to enact tighter regulations on EHRs and define when a patient's digital record would necessitate government oversight (Schulte and Fry, 2019b).

For the IoB technologies that fall under FDA oversight because they are medical devices, the FDA is promoting cybersecurity protections through an approach that distributes responsibility among different stakeholders. The agency also partners with hackers and medical device companies, e.g., at DEFCON's Biohacking Village, to find and disclose medical device vulnerabilities. The FDA and private advocacy groups have spearheaded numerous campaigns to better assess and protect the safety of implanted and connected medical devices. For example, since 2013, the FDA has held several public workshops designed to solicit and revise guidance, standards, and best practices for medical device cybersecurity (FDA, 2019c). It has also released pre- and post-market guidance documents in an effort to help device manufacturers understand how to identify and mitigate cybersecurity threats and vulnerabilities in their products (FDA, 2018d; FDA, 2016; FDA, 2005). These documents provide nonbinding guidance for how a device maker might meet FDA regulations for patient safety.

The FDA also posts advisory notices about known vulnerabilities in critical medical devices and supports an email distribution list that alerts users as issues become known (FDA, 2019a). Information sharing efforts have also been established with health information sharing analysis centers (H-ISAC) to facilitate the exchange of cybersecurity-related information between health-care providers and manufacturers. These two efforts help promote information awareness and transparency for consumers and other practitioners and may help, in the long run, improve overall security of these devices, although there is yet no evidence for this.

In addition, the FDA is working with the MITRE Corporation to develop a scoring system designed to rank the severity of software vulnerabilities in medical devices (Chase and Coley, 2019). While there already exists an industry standard for scoring software vulnerabilities in more traditional computing systems (see Common Vulnerability Scoring System SIG, undated), it is a blunt instrument and does not appropriately address the potential safety or health impacts on a patient whose medical device is hacked. This project will ensure that manufacturers and caregivers can more effectively assess and prioritize the risk of vulnerabilities.

Although the FDA is making strides in cybersecurity of medical devices, many IoB devices, especially those available for consumer use, do not fall under FDA jurisdiction.

Other Efforts

Federal and state officials have begun to address cybersecurity risks associated with IoB that are beyond FDA oversight, but there are few laws that mandate cybersecurity best practices. California is the first state to enact an IoT security law, SB-327, effective January 2020. The California law requires that a "manufacturer of a connected device . . . equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device." For example, it specifies that IoT devices may not have generic default passwords. Other states have debated IoT security legislation but have not passed bills. In March 2019, a bipartisan group of U.S. senators reintroduced the Internet of Things Cybersecurity Improvement Act of 2019, which attempts to improve security by documenting best practices for development, management, and patching of IoT devices, and recommends how the U.S. government can best apply these practices (Goodloe and Nandaraj Gallo, 2019). This bill, following up on past failed legislation, would mandate specific cybersecurity standards for IoT devices purchased by federal agencies with the hope that manufacturers might voluntarily adopt these for the commercial market.

An essential component in efforts to govern emerging technologies is public-private partnerships. For example, NIST collaborates with public and private partners to develop best practices and guidelines, such as its cybersecurity framework to manage cyber risk. The Medical Device Innovation Consortium (MDIC), a public-private partnership

between government and industry stakeholders, has championed efforts to foster a more collaborative industry dynamic in which researchers can disclose vulnerabilities in these medical devices without fear of civil liability or criminal prosecution (MDIC, 2018).[17] As of mid-2019, more than 20 organizations have established such programs (I Am the Cavalry, undated)

In addition to top-down cybersecurity governance efforts, several grassroots advocates have sought to promote cybersecurity best practices in connected medical devices. For instance, the nongovernment organization I Am the Cavalry has produced what it calls a Hippocratic Oath for Connected Medical Devices, with five voluntary principles that health-care providers and device manufacturers should adopt to better protect the safety and security of patients (Woods, Coravos, and Corman, 2019). The oath relates to ensuring that devices and the information contained on the devices are resilient against intrusion, compromise, tampering, and unauthorized disclosure, and that updates and other fixes will be prompt and effective.

Governance of IoB Data

As with IoB devices, there is no single entity that provides oversight to IoB data. Table 5 summarizes some of the primary entities and their responsibilities, though overall regulation of the privacy of personal information is fragmented across many state and federal agencies.[18]

Protection of medical information is regulated at the federal level, in part, by HIPAA. In the absence of other federal data privacy law, HIPAA provides the main framework for protecting IoB-related data. Specifically, the HIPAA Breach Notification Rule, 45 CFR §§ 164.400–414, requires that HIPAA-covered entities (health providers, health plans, and health-care clearinghouses) notify affected individuals when their personal health information has been accessed or disclosed in an improper way, such as when a hospital employee views a patient's record, or when a medical database is lost or stolen. The spirit of the regulation is to hold hospitals and practitioners accountable for lapses in data security practices and afford affected individuals an opportunity to more closely monitor their financial information and medical records to prevent financial or medical identity theft.[19] However, HIPAA does not cover nonmedical health or biometric information—indeed, it does not cover most of the data collected by consumer IoB devices.

The FTC helps ensure data security and consumer privacy through legal actions brought by the Bureau of Consumer Protection under Section 5(a) of the FTC act, which states that "unfair or deceptive acts or practices in or affecting commerce . . . are . . . declared unlawful." (15 U.S.C. Sec. 45[a][1]). This empowers the FTC to bring legal actions against companies that demonstrate a substantial lack of data security or privacy, or that are misleading about the way they use data. Given its oversight role, the FTC developed the *Mobile Health Apps Interactive Tool,* a checklist designed to help developers understand

TABLE 5
Selected Governance Responsibilities for IoB Data

Agency or Organization	Responsibility
U.S. Department of Health and Human Services Office for Civil Rights	Enforces Health Insurance Portability and Accounting Act (HIPAA)
U.S. Department of Health and Human Services Office of the National Coordinator for Health Information Technology	Coordinates efforts to ensure interoperability of health information, including EHRs
U.S. Federal Trade Commission (FTC)	Enforces data security and consumer privacy through Bureau of Consumer Protection
California Attorney General	Enforces California Consumer Privacy Act (CCPA)
Supervisory authorities in each European Union (EU) member state	Enforce GDPR to protect the personal information of EU residents

what laws may apply to their products. The FTC has brought actions against social media and other technology companies, but we found only a few examples of FTC actions against IoB developers.[20]

Data brokers are largely unregulated, but some legal experts are calling for policies to protect consumers. The Data Broker Accountability and Transparency Act was introduced to Congress in 2017 but gained no traction. In June 2019, 43 state attorneys general recommended another look at a 2014 FTC recommendation that Congress create a federal registry of all data brokers in the country (National Association of Attorneys General, 2019). Vermont became the first state to enact a law (Vermont Pub. L. H.764 [Act 171]) regulating data brokers, which became effective January 1, 2019. The law requires data brokers to register on a public database, specify the information that a customer cannot opt out of, explain options for what the customer can opt out of, and state whether a data breach has occurred within the past year. As of July 2019, Vermont is the only state to have enacted policies that make data broker activity more transparent.

Because the United States has no federal data privacy law, states have introduced a patchwork of laws and regulations that apply to residents' personal data, some of which includes IoB-related information. These laws differ greatly across states in terms of the types of information protected and available recourse, but overall, they seek to protect the confidentiality of consumer information and ensure that patients can access the information upon request, or to ensure that personal health information is used or shared only with patient approval (Smith, 2013).

Each U.S. state has a law requiring that private companies and government agencies notify individuals when their personal information has been accessed or disclosed in an unauthorized way, such as through a data breach ("Security Breach Notification Laws," 2018). While there is some variation regarding the conditions of notification, exceptions, and penalties, notification has become one of the main enforcement mechanisms for understanding and managing data breaches. As of July 1, 2019, 16 states had enacted laws that explicitly cover nonmedical biometric information in their data breach regulations, though each state varies in its definition of biometrics (based on Hennessy et al., 2019). Wisconsin is the only state to include DNA in its breach disclosure law as a specific protected data type distinct from biometric information (Wis. Stat. §134.98).

Illinois and Texas have passed laws regulating whether entities can capture or collect biometric information for commercial purposes without consent, limiting biometric information to "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry" (Illinois Biometric Information Privacy Act, 2019; Texas Business and Commerce Code, Title 11, Subtitle A, Chapter 503, 2009). Washington passed a law effective March 1, 2020, that requires entities to disclose capture and storage of biometric data for commercial purposes, to obtain consent, or to develop measures that prohibit subsequent selling of that information, where biometric data includes "unique biological patterns or characteristics . . . used to identify a specific individual" (Revised Code of Washington Chapter 19.375, 2019). At least a dozen other states have proposed similar biometric privacy legislation.

The CCPA, effective January 1, 2020, aims to improve customer privacy by giving individuals the right to know what information is collected about them, the purposes of that collection, and where that information is shared. Customers can also opt out of a business selling their personal data, and the law requires that businesses collecting personal information delete the record upon consumer request. *Personal data* in the CCPA is defined broadly and includes biometric information, geolocation data, and even inferences from the data used to build a psychological profile of the person. At least eight other states have drafted similar data privacy laws.

The European Union has enacted the GDPR, a collection of regulations designed to protect the personal information of EU residents, which also applies to software or hardware IoB developers and manufacturers. GDPR requires that users give informed consent prior to their personal information being collected, and that their information be protected at a level appropriate to the level of risk (harm) to the user. In addition, the GDPR gives EU citizens rights over the data that companies collect from them, including the right to access, delete, or transmit the data to other data controllers. Lawmakers in

Congress are working on regulations that would set a U.S. standard on consumer data protection and remedies akin to the GDPR or CCPA, but as of June 2019 have not enacted any policies (Ratnam, 2019).

The lack of consistency in IoB laws among states and between the state and federal level potentially enables regulatory gaps and enforcement challenges. As in many areas, rapid advancements in IoB technologies have outpaced the development of policy to address their risks. Such policies will require delicate navigation between the extremes of underregulation that fails to mitigate risks and overregulation that inhibits socially beneficial innovation or consumer adoption. Striking a balance between innovation and regulation will be imperative for protecting consumers while maintaining benefits and keeping the United States at the leading edge of this competitive field.

Looking Forward to Address Risk

This report has explored the complex and evolving IoB ecosystem and identified a variety of potential benefits and risks. A multitude of government and nongovernment stakeholders have a role in this ecosystem, and each stakeholder might take constructive steps toward addressing areas of risk. If these risks are not adequately addressed, the medical, health, and other benefits of IoB will not be fully realized.

Promoting National Security

IoB devices collect sensitive personal information that might be used by foreign adversaries to conduct espionage or interfere with values and practices important to Americans. Congress and the Executive Branch have specific roles in guarding against these risks. These efforts will need to extend beyond traditional national security policies to also grapple with new dynamics associated with the widespread use of IoB and threats from adversaries.

Had the events involving Strava or Vice President Cheney gone differently, the repercussions could have been enormous. Government departments can take these incidents as lessons learned on the risks presented by IoB and develop appropriate responses, as the Department of Defense did. For instance, guidelines on the use of IoB could be developed for high-ranking government officials.

As IoB usage spreads in authoritarian regimes, the U.S. Commerce Department can put foreign IoB companies on its "Entity List," preventing them from doing business with Americans, if those foreign companies are implicated in human rights violations. This has been done against Chinese entities that repress Uighur and other minority groups (Moss, 2019). CFIUS should also continue monitoring and investigating foreign investment in and acquisition of U.S. companies, especially those processing sensitive IoB data of Americans.

Threats to U.S. communication networks could increase as IoB gains popularity, so as 5G, Wi-Fi 6, and satellite internet standards are rolled out, the federal government should proactively fund studies and work with experts to develop security regulations.

Advancing Cybersecurity

All networked technologies have cybersecurity risk, but the sensitivity of IoB information and the potential medical and health impacts from disrupting or manipulating IoB are of acute concern. As described earlier, stakeholders have sought to promote cybersecurity best practices for parts of the IoB ecosystem, including through efforts led by the FDA, U.S. Department of Homeland Security, the Department of Commerce, and nongovernment organizations. However, not all IoB devices fall under FDA oversight, nor has the federal government instituted binding cybersecurity standards for IoB. There are opportunities to do more to promote IoB cybersecurity.

The federal government, including executive agencies and Congress, can first consider how to implement a risk management approach that establishes cybersecurity best practices and standards for the full range of IoB products. For example, an IoB-specific framework could be modeled after NIST's cybersecurity framework. This effort will be most effective if it is conducted in consultation with industry organizations and medical practitioners to ensure that the government fully understands

the technology and the attendant costs—including hindrances to innovation—of cybersecurity proposals. Importantly, an approach that considers the full range of IoB would go beyond existing FDA efforts to also include consumer health devices and EHRs. As part of this risk management approach, it will be important to consider how to incentivize quicker phase-out of the legacy medical devices with poor cybersecurity that are already in wide use. One possible step would be to develop and administer cybersecurity certifications for IoB (similar to an Energy Star label or nutritional value label) that, rather than mandating a certain minimal cybersecurity standard, would provide consumers with greater awareness of cybersecurity of products and thereby enable marketplace incentives for IoB device makers to follow specific cybersecurity guidelines ("How a Product Earns the ENERGY STAR Label," undated). This proposal, along with others, should be studied in collaboration with stakeholders.

In addition to government actors, health-care providers need to consider cybersecurity implications when they recommend or use the IoB. As a start, medical communities must continue to leverage cybersecurity expertise—for example, by using published guidelines that advise how to build a health-care cyber workforce.[21] Providers can also pledge to uphold the Hippocratic Oath for Connected Medical Devices, written by the grassroots organization I Am The Cavalry, which encourages health-care providers and stakeholders to recognize the importance of cybersecurity for patients.

Similarly, IoB developers must be more attentive to cybersecurity—for example, by following FDA cybersecurity guidelines (even if the device is not a medical device) and by integrating cybersecurity and privacy considerations from the beginning of product development. Device makers should test software for vulnerabilities often—including through use of vulnerability disclosure programs—and devise methods for users to patch software. In addition, device makers need to establish policies to notify and protect the consumer if cybersecurity or other issues arise (for instance, if the device needs to be patched or it will no longer be supported by the manufacturer). This effort will need to consider and address the unique challenges of cybersecurity for IoB—for instance, the challenge of patching devices that are implanted and cannot be easily recalled. Other cybersecurity best practices for IoB include threat modeling, data storage standards, and keeping a repository of software source code that can be reviewed by independent cybersecurity researchers.

Ensuring Privacy

The United States does not have a comprehensive federal data privacy law, and much of the data collected by IoB is not regulated by existing state law. These are complex policy areas, and the range of IoB is vast, so a single policy that can address them all is not likely. To address the risks to privacy from IoB devices, Congress should consider establishing federal data transparency and protection standards for data that are collected from them. As it stands, consumers have limited ability to identify who is storing their intimate health and other data and how those data are being used—so, as a starting point for regulation, government entities can take steps to ensure greater transparency about data collection practices. As the consequences from such regulations as GDPR and CCPA emerge, Congress can take lessons learned from both their successes and failures to consider how to give IoB users rights over their personal information, including the right to opt out of collection. Federal and state governments might also consider regulations for data brokers, restrictions on who can collect data, how such information is used, whether it is sold to third parties, and so forth.

There is also a role for the federal government to harmonize the patchwork of state laws regarding data breaches and health information through a federal data breach notification standard. The federal government can encourage and fund independent research on such emerging issues as data endurance, posthumous privacy, and the right to be forgotten regarding IoB data. Rules also need to be established for how insurers, employers, or others are permitted to use IoB data.

Authorities and resources for privacy in health and IoB data are shared among a variety of government organizations, including the FTC, NIST, and Health and Human Services (of which the FDA is a part). Congress needs to decide what subset of these

organizations would be best suited to enforce privacy violations and data protection policies regarding IoB devices. Additional resources may need to be allocated so that sufficient support is available to enforce regulations as IoB products become more widespread. For example, as it stands, the FTC has only 40 full-time personnel dedicated to data privacy (compared with 500 in the UK's data protection authority), and FTC Chairman Joseph Simons has stated that the agency is not sufficiently resourced to increase its data privacy enforcement (Simons, 2019).

Raising Awareness

The rapid evolution of IoB has created an environment in which consumers may be unwittingly using IoB and where there is confusion and lack of clarity about its benefits and potential ethical downsides. The IoB ecosystem may not be as useful to medical providers or consumers as it might appear, at least in the short term. For instance, some studies have shown that constant tracking of biometric activity through health apps, such as sleep trackers, can increase users' anxiety and worsen conditions such as insomnia (Baron et al., 2017; Zraick and Mervosh, 2019). Many IoB technologies have not yet developed a clinical evidence base on long-term outcomes. Stakeholders will need to research and promulgate information regarding the realistic and pragmatic benefits of IoB as it becomes more mainstream, and also where harms will likely emerge.

The FTC already plays an important role regarding the marketing of IoB technologies,[22] and there are opportunities for the FTC to play a larger role to ensure that marketing claims about improved well-being or specific health treatment are backed by appropriate evidence. However, the FTC may need additional resources to grapple with the broad range of IoB technologies that have hit the marketplace in recent years, and additional personnel with expertise in IoB will be important to ensure that IoB developers' claims are not deceptive or unfair.

There are also opportunities to increase awareness of the ethical implications of IoB, for instance through additional federal or foundation funding of research related to disparities associated with IoB data collection and health care. This research can also focus on the extent to which IoB infringes on autonomy in the workplace or otherwise undermines reasonable expectations for anonymity or privacy.

Federal and state governments can also work with partners to develop guidelines for responsible development and marketing of IoB. State governments can collaborate with thought leaders at universities and other institutions to tap expertise in IoB-related policy topics, such as cybersecurity and digital health.[23] These types of partnerships between decisionmakers and experts can help identify gaps in the regulatory system, foster innovation in technology development, and protect all stakeholders.

Even in the absence of a regulatory forcing function, IoB developers can be clearer with consumers about cybersecurity risks and data privacy practices associated with their products. IoB developers are collecting vast amounts of intimate data, and they need to clearly state privacy policies and obtain informed consent for their collection practices. These policies should straightforwardly explain how data will be protected, how these data will be used, and with whom they may be shared. Developers should also educate the public about the risks associated with IoB products.

Lastly, patients and consumers need to recognize the risks of IoB and consider these risks when deciding to use such devices. In the absence of new regulations, consumers should be wary and proceed under the assumption that, once data are collected by an IoB device, the consumer will not likely have complete control over how those data are stored and used and should be prepared for them to be potentially breached or otherwise widely shared. Ultimately, consumers need to be aware that their intimate data are collected by entities that do not necessarily have consumers' best interests in mind. Increased awareness of the IoB ecosystem and its risks is critical.

Notes

1 One definition of the IoB, put forth by Matwyshyn, is "the creeping reliance of human bodies on software, hardware, and the internet for key aspects of their functionality" (The Internet of Bodies, 2018). Three generations of IoB are defined: body-external, body-internal, and body-melded (Matwyshyn, 2019).

2 We restrict our definition of IoB devices to technologies that can be linked to an individual rather than to technologies that are linked to traits more or less universal to all humans or a particular disease. Therefore, large genetic sequence databases (such as GenBank) are not considered IoB data, and techniques (such as CRISPR) that are enabled by such databases are not considered IoB technologies.

3 The FDA defines a *medical device* as follows (FDA, 2018a):

- an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part or accessory which is: recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them,
- intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or
- intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of any of its primary intended purposes.

4 A concept related to IoT and IoB is cyber-physical systems. According to the Networking and Information Technology Research and Development (NITRD), cyber-physical systems are "smart networked systems with embedded sensors, processors and actuators that are designed to sense and interact with the physical world (including the human users)" (NITRD, 2015).

5 There are numerous additional terms not described here that relate to IoB—such as human enhancement technologies, DIYbio (do-it-yourself biology), wetware (direct brain-computer connections), and quantified self—that are part of this growing field of body-connected technologies.

6 We define *freestanding devices* as those that stand and operate on their own, free of continuous bodily attachment.

7 The new Wi-Fi 6 standard, also referred to as 802.11ax, is under development and expected to have final approval in June 2020 ("Official IEEE 802.11 Working Group Project Timelines," 2019).

8 An attack surface is the set of all potential entry points that could be used to attack a system (Manadhata and Wing, 2010).

9 However, the safety risks of computer-controlled medical devices dates back to at least 1985 (Leveson, 1995).

10 This document is not publicly available.

11 This is likely an underestimate of the actual number of known vulnerabilities, because this list likely does not capture all vulnerabilities from software libraries that are designed for other products but used in these systems.

12 2019 data were not included.

13 The right to be forgotten is part of the European Union's General Data Protection Regulation (GDPR), but as of June 2019, it can be enforced only within the European Union.

14 Currently, the legal right to privacy applies to living persons and not deceased ones (Banta, 2016). HIPAA privacy rules are upheld for 50 years after the decedent's death (U.S. Department of Health and Human Services, 2013).

15 As argued in one study on the ethics of human enhancement, "assimilating tools into our persons creates an intimate or enhanced connection with our tools" (Allhoff et al., 2010).

16 There are several other organizations that have equities in the overall safety of IoB and IoT devices, such as the Consumer Product Safety Commission, but a full discussion of all relevant bodies is beyond the scope of this work.

17 Safe disclosure of software vulnerabilities is a luxury researchers have not always enjoyed. Fortunately, there is a growing movement to nurture an open and transparent process for notification by researchers to vendors.

18 A full discussion of privacy regulation is beyond the scope of this work; however, see Mulligan, Freeman, and Linebaugh (2019).

19 However, it is unproven whether this rule has improved data security practices.

20 One example is described in Morris (2017).

21 One example is the "Healthcare Industry Cybersecurity Workforce Guide" (Healthcare and Public Health Sector Coordinating Council, undated). Another example, not specifically for healthcare organizations, is NIST's "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework" (Newhouse et al., 2017).

22 The FTC is not the only organization involved here; the FDA, for instance, regulates the marketing of medical devices.

23 For example, the Center for Body Computing at the University of Southern California has partnered with the California Governor's Office of Business and Economic Development to develop and disseminate concepts of cybersecurity in health-care information technology (University of Southern California Center for Body Computing, 2018).

References

Agboola, Stephen, Kamal Jethwani, Kholoud Khateeb, Stephanie Moore, and Joseph Kvedar, "Heart Failure Remote Monitoring: Evidence from the Retrospective Evaluation of a Real-World Remote Monitoring Program," *Journal of Medical Internet Research*, Vol. 17, No. 4, 2015, p. e101.

Agniel, Denis, Isaac S. Kohane, and Griffin M. Weber, "Biases in Electronic Health Record Data Due to Processes Within the Healthcare System: Retrospective Observational Study," *BMJ*, Vol. 361, 2018, p. k1479.

Allen, Marshall, "Health Insurers Are Vacuuming up Details About You—and It Could Raise Your Rates," *ProPublica*, July 17, 2018a. As of July 3, 2019: https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates

———, "You Snooze, You Lose: Insurers Make the Old Adage Literally True," *ProPublica*, November 21, 2018b. As of April 27, 2020: https://www.propublica.org/article/you-snooze-you-lose-insurers-make-the-old-adage-literally-true

Allen-Graham, Judith, Lauren Mitchell, Natalie Heriot, Roksana Armani, David Langton, Michele Levinson, Alan Young, Julian A. Smith, Tom Kotsimbos, and John W. Wilson, "Electronic Health Records and Online Medical Records: An Asset or a Liability Under Current Conditions?" *Australian Health Review*, Vol. 42, No. 1, 2018, pp. 59–65.

Allhoff, Fritz, Patrick Lin, James Moor, and John Weckert, "Ethics of Human Enhancement: 25 Questions & Answers," *Studies in Ethics, Law, and Technology*, Vol. 4, No. 1, 2010, p. Article-4.

Apple, "ECG App and Irregular Heart Rhythm Notification Available Today on Apple Watch," press release, December 6, 2018.

Appleby, Julie, "A Wake-up Call on Smart Beds and Sleep Apps That Collect Your Data," *Time*, May 29, 2019. As of April 27, 2020: https://time.com/5592792/a-wake-up-call-on-smart-beds-and-sleep-apps-that-collect-your-data/

Atlantic Council, *Cyber Risk Thursday: Internet of Bodies*, webcast, September 21, 2017. As of April 27, 2020: https://www.atlanticcouncil.org/unused/webcasts/cyber-risk-thursday-internet-of-bodies/

Axon A. I. and Policing Technology Ethics Board, *First Report of the Axon AI & Policing Technology Ethics Board*, June 2019. As of April 27, 2020: https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5d13d7e1990c4f00014c0aeb/1561581540954/Axon_Ethics_Board_First_Report.pdf

Baenen, Jeff, "Wisconsin Company Holds 'Chip Party' to Microchip Workers," *Chicago Tribune*, August 2, 2017. As of April 27, 2020: https://www.chicagotribune.com/business/blue-sky/ct-wisconsin-company-microchips-workers-20170801-story.html

Banta, Natalie M., *Death and Privacy in the Digital Age*, North Carolina Law Review, Vol. 94, No. 3, 2016 p. 927. As of April 27, 2020: https://scholarship.law.unc.edu/nclr/vol94/iss3/4/

Baron, Kelly Glazer, Sabra Abbott, Nancy Jao, Natalie Manalo, and Rebecca Mullen, "Orthosomnia: Are Some Patients Taking the Quantified Self Too Far?" *Journal of Clinical Sleep Medicine*, Vol. 13, No. 2, 2017, pp. 351–354. As of April 27, 2020: http://jcsm.aasm.org/viewabstract.aspx?pid=30955

Bauerle Danzman, Sarah, and Geoffrey Gertz, "Why Is the U.S. Forcing a Chinese Company to Sell the Gay Dating App Grindr?" *Washington Post*, April 3, 2019. As of April 27, 2020: https://www.washingtonpost.com/politics/2019/04/03/why-is-us-is-forcing-chinese-company-sell-gay-dating-app-grindr/?noredirect=on&utm_term=.6ca317886ff3

Beardsley, Tod, "R7-2016-07: Multiple Vulnerabilities in Animas OneTouch Ping Insulin Pump," *Rapid7* blog, 2016. As of April 27, 2020: https://blog.rapid7.com/2016/10/04/r7-2016-07-multiple-vulnerabilities-in-animas-onetouch-ping-insulin-pump/

Bentley, Daniel, "This Hospital Bed Can Save Lives," *Fortune*, March 20, 2018. As of April 27, 2020: https://fortune.com/2018/03/20/earlysense-hospital-bed/

Binnendijk, Annika, Robert Timothy Marler, and Elizabeth M. Bartels, *Brain-Computer Interfaces: U.S. Military Applications and Implications, An Initial Assessment*, Santa Monica, Calif.: RAND Corporation, RR-2996-RC, forthcoming.

Boughton, C. K., and R. Hovorka, "Is an Artificial Pancreas (Closed-Loop System) for Type 1 Diabetes Effective?" *Diabetic Medicine*, Vol. 36, No. 3, 2019, pp. 279–286.

Bowcott, Owen, "'Right to Be Forgotten' Could Threaten Global Free Speech, Say NGOs," *The Guardian*, September 9, 2018. As of April 27, 2020: https://www.theguardian.com/technology/2018/sep/09/right-to-be-forgotten-could-threaten-global-free-speech-say-ngos

Braveman, Paula, Catherine Cubbin, Susan Egerter, Sekai Chideya, Kristen Marchi, Marilyn Metzler, and Samuel Posner, "Socioeconomic Status in Health Research: One Size Does Not Fit All," *Journal of the American Medical Assocation*, Vol. 294, No. 22, 2005, pp. 2879–2888.

Brown, Dalvin, "Hacking Diabetes: People Break into Insulin Pumps as an Alternative to Delayed Innovations," *USA Today*, June 5, 2019. As of April 27, 2020: https://www.wired.com/2014/12/diabetes-patients-hacking-together-diy-bionic-pancreases/

Bryan-Low, Cassell, Colin Packham, David Lague, Steve Stecklow, and Jack Stubbs, "Hobbling Huawei: Inside the U.S. War on China's Tech Giant," Reuters, May 21, 2019. As of April 27, 2020: https://www.reuters.com/investigates/special-report/huawei-usa-campaign/

Bushatz, Amy, "Army Issues FitBit Bands in Test Fitness Program," press release, Military.com, October 22, 2013. As of April 27, 2020: https://www.military.com/daily-news/2013/10/22/army-issues-fitbit-bands-in-test-fitness-program.html

Callahan, Daniel, *Bioethics Briefing Book for Journalists, Policymakers, and Campaigns: Health Care Costs and Medical Technology*, Garrison, N.Y.: The Hastings Center, 2008. As of April 27, 2020: https://www.thehastingscenter.org/briefingbook/health-care-costs-and-medical-technology/

Caplan, Arthur L., and Phoebe Friesen, "Health Disparities and Clinical Trial Recruitment: Is There a Duty to Tweet?" *PLoS Biology*, Vol. 15, No. 3, 2017, p. e2002040.

Center for Internet Security, "EI-ISAC Cybersecurity Spotlight—CIA Triad," webpage, undated. As of April 27, 2020: https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-cia-triad/

Chase, Penny, and Steve Christey Coley, "Rubric for Applying CVSS to Medical Devices," MITRE Corp., January 16, 2019.

Chen, Xing, Babak Assadsangabi, York Hsiang, and Kenichi Takahata, "Enabling Angioplasty-Ready 'Smart' Stents to Detect in-Stent Restenosis and Occlusion," *Advanced Science*, Vol. 5, No. 5, 2018, p. 1700560.

Clymo, Rob, "In-Car AI Could Soon Know If You're Having a Good or Bad Day," *TechRadar*, October 4, 2018. As of April 27, 2020: https://www.techradar.com/news/in-car-ai-could-soon-know-if-youre-having-a-good-or-bad-day

Coates McCall, Iris, Chloe Lau, Nicole Minielly, and Judy Illes, "Owning Ethical Innovation: Claims About Commercial Wearable Brain Technologies," *Neuron*, Vol. 102, No. 4, May 22, 2019, pp. 728–31.

"Common Vulnerability Scoring System SIG," webpage, FIRST, Cary, N.C., undated. As of April 27, 2020: https://www.first.org/cvss/

Copp, Tara, "Fitbits and Fitness-Tracking Devices Banned for Deployed Troops," *Military Times*, August 6, 2018. As of April 27, 2020: https://www.militarytimes.com/news/your-military/2018/08/06/devices-and-apps-that-rely-on-geolocation-restricted-for-deployed-troops/

CPDP Conferences, "CPDP 2018: The Internet of (Vulnerable) Bodies," YouTube video, Computers, Privacy and Data Protection, February 6, 2018. As of April 28, 2020: https://www.youtube.com/watch?v=10Rlk8uj-lo

Das, Ashok Kumar, Sherali Zeadally, and Mohammad Wazid, "Lightweight Authentication Protocols for Wearable Devices," *Computers & Electrical Engineering*, Vol. 63, 2017, pp. 196–208. As of May 13, 2020: https://www.sciencedirect.com/science/article/pii/S0045790617305347#bib0009

Day, Matt, "Amazon Is Working on a Device That Can Read Human Emotions," Bloomberg, May 23, 2019. As of April 28, 2020: https://www.bloomberg.com/news/articles/2019-05-23/amazon-is-working-on-a-wearable-device-that-reads-human-emotions

Defense Intelligence Agency, "Challenges to Security in Space," press release, February 11, 2019. As of April 28, 2020: https://media.defense.gov/2019/Feb/11/2002088710/-1/-1/1/SPACE-SECURITY-CHALLENGES.PDF

Deichmann, Johannes, Kersten Heineke, Thomas Reinbacher, and Dominik Wee, "Creating a Successful Internet of Things Data Marketplace," McKinsey Digital, October 2016. As of July 3, 2019: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/creating-a-successful-internet-of-things-data-marketplace

Derousseau, Ryan, "The Tech That Tracks Your Movements at Work," BBC News, June 14, 2017. As of April 28, 2020: https://www.bbc.com/worklife/article/20170613-the-tech-that-tracks-your-movements-at-work

Dinh-Le, Catherine, Rachel Chuang, Sara Chokshi, and Devin Mann, "Wearable Health Technology and Electronic Health Record Integration: Scoping Review and Future Directions," *JMIR Mhealth Uhealth*, Vol. 7, No. 9, 2019, p. e12861.

Doffman, Zak, "New Pentagon Laser Identifies High-Risk Individuals by Their Heartbeat," *Forbes*, June 27, 2019. As of April 28, 2020: https://www.forbes.com/sites/zakdoffman/2019/06/27/u-s-military-laser-can-identify-people-by-their-heartbeats-mit-reports/#6e40b06b2dc6

Dolley, Shawn, "Big Data's Role in Precision Public Health," *Frontiers in Public Health*, Vol. 6, 2018, p. 68.

Donahue, Michelle, "How a Color-Blind Artist Became the World's First Cyborg," *National Geographic*, April 3, 2017. As of April 28, 2020: https://news.nationalgeographic.com/2017/04/worlds-first-cyborg-human-evolution-science/

Downey, C. L., S. Chapman, R. Randell, J. M. Brown, and D. G. Jayne, "The Impact of Continuous Versus Intermittent Vital Signs Monitoring in Hospitals: A Systematic Review and Narrative Synthesis," *International Journal of Nursing Studies*, Vol. 84, 2018, pp. 19–27.

Edinburgh Law School, *MacCormick Fellow Seminar: Prof Andrea Matwyshyn*, YouTube video, October 23, 2018. As of April 28, 2020: https://www.youtube.com/watch?v=7Cs0yc9u-VE

Emondi, Al, "Next-Generation Nonsurgical Neurotechnology," Defense Advanced Research Projects Agency, webpage, undated. As of April 28, 2020: https://www.darpa.mil/program/next-generation-nonsurgical-neurotechnology

Entzeridou, Eleni, Evgenia Markopoulou, and Vasiliki Mollaki, "Public and Physician's Expectations and Ethical Concerns About Electronic Health Record: Benefits Outweigh Risks Except for Information Security," *International Journal of Medical Informatics*, Vol. 110, 2018, pp. 98–107.

Etherington, Darrell, "Elon Musk's Neuralink Looks to Begin Outfitting Human Brains with Faster Input and Output Starting Next Year," *TechCrunch*, July 16, 2019. As of April 28, 2020: https://techcrunch.com/2019/07/16/elon-musks-neuralink-looks-to-begin-outfitting-human-brains-with-faster-input-and-output-starting-next-year/

Faiola, Anthony, and Richard J. Holden, "Consumer Health Informatics: Empowering Healthy-Living-Seekers Through mHealth," *Progress in Cardiovascular Diseases*, Vol. 59, No. 5, 2017, pp. 479–486.

Fanucci, Luca, Sergio Saponara, Tony Bacchillone, Massimiliano Donati, Pierluigi Barba, Isabel Sanchez-Tato, and Cristina Carmona, "Sensing Devices and Sensor Signal Processing for Remote Monitoring of Vital Signs in CHF Patients," IEEE *Transactions on Instrumentation and Measurement*, Vol. 62, 2013, pp. 553–569.

Farivar, Cyrus, "'Stop the Cyborgs' Launches Public Campaign Against Google Glass," *Ars Technica*, March 22, 2013. As of July 9, 2019: https://arstechnica.com/tech-policy/2013/03/stop-the-cyborgs-launches-public-campaign-against-google-glass/

FDA—*See* U.S. Food and Drug Administration.

Federal Trade Commission,"Complying with the FTC's Health Breach Notification Rule," webpage, April 2010. As of April 28, 2020:
https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule

———, "Careful Connections: Building Security in the Internet of Things," webpage, January 2015. As of April 28, 2020:
https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf

FTC—*See* Federal Trade Commission.

Garg, Satish K., Stuart A. Weinzimer, William Tamborlane, Bruce A. Buckingham, Bruce W. Bode, Timothy S. Bailey, Ronald L. Brazg, Jacob Illany, Robert H. Slover, Stacey M. Anderson, Richard M. Bergenstal, Benyamin Grosman, Anirban Roy, Toni L. Cordero, John Shin, Scott W. Lee, and Francine R. Kaufman, "Glucose Outcomes with the In-Home Use of a Hybrid Closed-Loop Insulin Delivery System in Adolescents and Adults with Type 1 Diabetes," *Diabetes Technology & Therapeutics*, Vol. 19, No. 3, 2017, pp. 155–163.

Geller, Stacie E., Abby Koch, Beth F. Pellettiere, and Molly Carnes, "Inclusion, Analysis, and Reporting of Sex and Race/Ethnicity in Clinical Trials: Have We Made Progress?" *Journal of Women's Health*, Vol. 20, No. 3, 2011, pp. 315–320.

Geller, Stacie E., Abigail R. Koch, Pamela Roesch, Amarette Filut, Emily Hallgren, and Molly Carnes, "The More Things Change, the More They Stay the Same: A Study to Evaluate Compliance with Inclusion and Assessment of Women and Minorities in Randomized Controlled Trials," *Academic Medicine*, Vol. 93, No. 4, 2018, pp. 630–635.

Gillan, Fraser, "The Transhumanists Who Are 'Upgrading' Their Bodies," BBC News, October 6, 2019. As of November 11, 2019:
https://www.bbc.com/news/uk-scotland-49893869

Giuliano, Karen, Wan-Ting Su, Daniel Degnan, Kristy Fitzgerald, Richard Zink, and Poching DeLaurentis, "Intravenous Smart Pump Drug Library Compliance: A Descriptive Study of 44 Hospitals," *Journal of Patient Safety*, Vol. 14, No. 4, 2018, pp. e76–e82.

Glasgow, Russell E., Bethany M. Kwan, and Daniel D. Matlock, "Realizing the Full Potential of Precision Health: The Need to Include Patient-Reported Health Behavior, Mental Health, Social Determinants, and Patient Preferences Data," *Journal of Clinical and Translational Science*, Vol. 2, No. 3, 2018, pp. 183–185.

Gonzales, Amy, "Is Digital Technology Making Health Inequality Worse?" *Interdisciplinary Association for Population Health Science*, November 20, 2017. As of April 28, 2020:
https://iaphs.org/digital-technology-making-health-inequality-worse/

Goodin, Dan, "Serious Flaws Leave WPA3 Vulnerable to Hacks That Steal Wi-Fi Passwords," *Ars Technica*, April 11, 2019. As of April 28, 2020:
https://arstechnica.com/information-technology/2019/04/serious-flaws-leave-wpa3-vulnerable-to-hacks-that-steal-wi-fi-passwords/

Goodloe, Katharine, and Micha Nandaraj Gallo, "Senate Reintroduces IoT Cybersecurity Improvement Act," *Inside Privacy*, March 12, 2019. As of July 3, 2019:
https://www.insideprivacy.com/internet-of-things/senate-reintroduces-iot-cybersecurity-improvement-act/

Griffin, Patrick, "Edit Thyself: Biohacking in the Age of CRISPR," in *Science in the News*, February 14, 2018. As of April 28, 2020:
http://sitn.hms.harvard.edu/flash/2018/edit-thyself-biohacking-age-crispr/

Groll, Elias, "The Enduring Mystery of Who Hacked Anthem," *Foreign Policy*, May 10, 2019. As of April 28, 2020:
https://foreignpolicy.com/2019/05/10/the-enduring-mystery-of-who-hacked-anthem-hackers-spies-china/

Grush, Loren, "SpaceX is in Communication with All But Three of 60 Starlink Satellites One Month After Launch," *The Verge*, June 28, 2019. As of April 28, 2020:
https://www.theverge.com/2019/6/28/19154142/spacex-starlink-60-satellites-communication-internet-constellation

Gryphon Scientific and Rhodium Group, *China's Biotechnology Development: The Role of US and Other Foreign Engagement*, Washington, D.C.: U.S.-China Economic and Security Review Commission, February 14, 2019. As of April 28, 2020:
https://www.uscc.gov/Research/china%E2%80%99s-biotechnology-development-role-us-and-other-foreign-engagement

Gutierrez, Erie G., Nathan E. Crone, Joon Y. Kang, Yaretson I. Carmenate, and Gregory L. Krauss, "Strategies for Non-EEG Seizure Detection and Timing for Alerting and Interventions with Tonic–Clonic Seizures," *Epilepsia*, Vol. 59, 2018, pp. 36–41.

Hambling, David, "The Pentagon Has a Laser That Can Identify People from a Distance—by Their Heartbeat," *MIT Technology Review*, June 27, 2019. As of April 28, 2020:
https://www.technologyreview.com/s/613891/the-pentagon-has-a-laser-that-can-identify-people-from-a-distanceby-their-heartbeat/

Harper, Sarah, *Ageing Societies: Myths, Challenges and Opportunities*, London: Hodder Education, 2006.

Haskins, Caroline, "Revealed: This Is Palantir's Top-Secret User Manual for Cops," *Motherboard*, July 12, 2019. As of July 15, 2019:
https://www.vice.com/en_us/article/9kx4z8/revealed-this-is-palantirs-top-secret-user-manual-for-cops

Healey, Jason, Neal Pollard, and Beau Woods, "The Healthcare Internet of Things: Risks and Rewards," Atlantic Council, March 2015. As of July 13, 2019:
https://www.atlanticcouncil.org/images/publications/ACUS_Intel_MedicalDevices.pdf

Healthcare and Public Health Sector Coordinating Council, "Healthcare Industry Cybersecurity Workforce Guide: Recruiting and Retaining Skilled Cybersecurity Talent," undated. As of August 30, 2019:
https://healthsectorcouncil.org/wp-content/uploads/2019/06/Healthcare-Industry-Cybersecurity-Workforce-Guide-1.pdf

Hennessy, Jennifer J., Chanley T. Howell, Michael R. Overly, Jennifer L. Rathburn, Steven M. Millendorf, Aaron K, Tantleff, Samuel D. Goldstick, and Thomas E. Chisena, "State Data Breach Notification Laws," webpage, Foley & Lardner LLP, updated January 2019. As of April 28, 2020:
https://www.foley.com/en/insights/publications/2019/01/state-data-breach-notification-laws

Hern, Alex, "Fitness Tracking App Strava Gives Away Location of Secret US Army Bases," *The Guardian*, January 28th, 2018. As of April 28, 2020:
https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

HHS—*See* U.S. Department of Health and Human Services.

Holley, Peter, "Wearable Technology Started by Tracking Steps. Soon, It May Allow Your Boss to Track Your Performance," *Washington Post*, June 28, 2019. As of July 3, 2019: https://www.washingtonpost.com/technology/2019/06/28/wearable-technology-started-by-tracking-steps-soon-it-may-allow-your-boss-track-your-performance/?utm_term=.c7692bb4b23a

"How a Product Earns the ENERGY STAR Label," webpage, U.S. Department of Environmental Protection, U.S. Department of Energy, undated. As of April 28, 2020: https://www.energystar.gov/products/how-product-earns-energy-star-label

"How Insulin Pumps Work," webpage, Diabetes.co.uk, Diabetes Digital Media, January 15, 2019. As of April 28, 2020: https://www.diabetes.co.uk/insulin/how-insulin-pumps-work.html

Hurley, Dan, "Diabetes Patients Are Hacking Their Way Toward a Bionic Pancreas," *Wired*, December 24, 2014. As of April 28, 2020: https://www.wired.com/2014/12/diabetes-patients-hacking-together-diy-bionic-pancreases/

I Am the Cavalry, "Disclosure Programs," webpage, undated. As of April 28, 2020: https://www.iamthecavalry.org/resources/disclosure-programs/

Illinois General Assembly, Biometric Information Privacy Act, 740 Illinois Compiled Statutes 14/1. As of July 3, 2019: http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

"Imagining a New Interface: Hands-Free Communication Without Saying a Word," webpage, Tech@Facebook, July 30, 2019. As of April 28, 2020: https://tech.fb.com/imagining-a-new-interface-hands-free-communication-without-saying-a-word/

International Data Corporation, "The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast," June 18, 2019. As of April 28, 2020: https://www.idc.com/getdoc.jsp?containerId=prUS45213219

Jackson, James K., "The Committee on Foreign Investment in the United States (CFIUS)," Congressional Research Service, RL33388, October 23, 2019. As of April 28, 2020: https://crsreports.congress.gov/product/pdf/RL/RL33388

Jamoon, Eric, Vaishali Patel, Jennifer King, and Michael Furukawa, "National Perceptions of EHR Adoption: Barriers, Impacts, and Federal Policies," 2012 National Conference on Health Statistics, Washington, D.C., August 6–8, 2012.

Jaramillo, Estrella, "Meet the Women's Health Companies Disrupting the Wearable Space," *Forbes*, May 16, 2019. As of April 28, 2020: https://www.forbes.com/sites/estrellajaramillo/2019/05/16/womens-health-companies-disrupting-the-wearable-space/#4d36fdb228b3

Kastrenakes, Jacob, "Wi-Fi 6: Is It Really That Much Faster?" *The Verge*, February 21, 2019. As of April 28, 2020: https://www.theverge.com/2019/2/21/18232026/wi-fi-6-speed-explained-router-wifi-how-does-work

Khan, Sieeka, "Electronic Tattoos Can Be Made Through Graphene and Silk," *Science Times*, March 13, 2019. As of April 28, 2020: https://www.sciencetimes.com/articles/18598/20190313/electronic-tattoos-made-through-graphene-silk.htm

Klitzman, Robert, *Am I My Genes?: Confronting Fate and Family Secrets in the Age of Genetic Testing*, Oxford, UK: Oxford University Press, 2012.

Knack, Anna, Advait Deshpande, Stijn Hoorens, and Salil Gunashekar, "Wearable Devices: Implications of Game-Changing Technologies in the Services Sector in Europe," *Eurofound*, 2019. As of April 28, 2020: https://www.rand.org/pubs/external_publications/EP67914.html

Kumar, Shefaili, J. Tran Tran, Wei-Nchih Lee, Ben Bradshaw, Luca Foschini, and Jessie Juusola, "Longitudinal Data from Activity Trackers Show That Those with Greater Inconsistency in Activity Levels are More Likely to Develop More Severe Depression," *Value in Health*, Vol. 21, 2018, p. S191.

Lai, A. M., P. Y. S. Hsueh, Y. K. Choi, and R. R. Austin, "Present and Future Trends in Consumer Health Informatics and Patient-Generated Health Data," *Yearbook of Medical Informatics*, Vol. 26, No. 01, 2017, pp. 152–159.

Larson, Erik, "Chinese Citizen Indicted in Anthem Hack of 80 Million People," Bloomberg News, May 9, 2019. As of April 28, 2020: https://www.bloomberg.com/news/articles/2019-05-09/chinese-national-indicted-by-u-s-grand-jury-over-anthem-hack

Lee, Mary, "The 'Internet of Bodies' is Setting Dangerous Precedents," *Washington Post*, October 15, 2018. As of July 13, 2019: https://www.washingtonpost.com/news/theworldpost/wp/2018/10/15/health-data/?utm_term=.ff1d3a1de516

LeMoyne, Robert, Timothy Mastroianni, Donald Whiting, and Nestor Tomycz, *Wearable and Wireless Systems with Internet Connectivity for Quantification of Parkinson's Disease and Essential Tremor Characteristics*, Vol. 31, Wearable and Wireless Systems for Healthcare II, Singapore: Springer, 2019.

Leveson, Nancy G., *Safeware: System Safety and Computers*, Boston, Mass.: Addison-Wesley, 1995.

Lilley, Kevin, "20,000 Soldiers Tapped for Army Fitness Program's 2nd Trial," *Army Times*, July 27th, 2015. As of April 28, 2020: https://www.armytimes.com/news/your-army/2015/07/27/20000-soldiers-tapped-for-army-fitness-program-s-2nd-trial/

Linder, Courtney, "Why This Software Engineer Implanted a Tesla Valet Key into Her Arm," *Popular Mechanics*, August 14, 2019. As of April 28, 2020: https://www.popularmechanics.com/technology/infrastructure/a28698503/tesla-key-implant/

Lupton, Deborah, "Quantifying the Body: Monitoring and Measuring Health in the Age of Mhealth Technologies," *Critical Public Health*, Vol. 23, No. 4, 2013, pp. 393–403.

———, "Critical Perspectives on Digital Health Technologies," *Sociology Compass*, Vol. 8, No. 12, 2014, pp. 1344–1359.

MacMillan, Douglas, "Data Brokers Are Selling Your Secrets. How States Are Trying to Stop Them," *Washington Post*, June 24, 2019. As of July 3, 2019: https://www.washingtonpost.com/business/2019/06/24/data-brokers-are-getting-rich-by-selling-your-secrets-how-states-are-trying-stop-them/?utm_term=.a46f70fcae28

Manadhata, Pratyusa K., and Jeannette M. Wing, "An Attack Surface Metric," *IEEE Transactions on Software Engineering*, Vol. 37, No. 3, 2010, pp. 371–386.

Marmot, Michael, "Social Determinants of Health Inequalities," *The Lancet*, Vol. 365, No. 9464, 2005, pp. 1099–1104.

Marr, Bernard, "How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read," *Forbes*, May 21, 2018. As of August 30, 2019: https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#2df2278360ba

———, "Artificial Intelligence in Your Toilet. Yes, Really!" *Forbes*, May 20, 2019a. As of April 28, 2020: https://www.forbes.com/sites/bernardmarr/2019/05/20/artificially-intelligent-toilets-yes-they-are-here/2/#477336615a85

———, "Chinese Social Credit Score: Utopian Big Data Bliss or Black Mirror on Steroids?" *Forbes*, January 21, 2019b. As of April 28, 2020: https://www.forbes.com/sites/bernardmarr/2019/01/21/chinese-social-credit-score-utopian-big-data-bliss-or-black-mirror-on-steroids/

Massachusetts Institute of Technology Media Lab, "Project AttentivU," press release, August 20, 2019. As of August 30, 2019: https://www.media.mit.edu/projects/attentivu/overview/

Matwyshyn, Andrea M., "The Internet of Bodies," *9th Annual Privacy Law Scholars Conference, Berkeley Center for Law & Technology*, Washington, D.C., June 2, 2016. As of April 28, 2020: https://www.law.berkeley.edu/research/bclt/past-events/2016-conferences/june-2016-the-9th-annual-privacy-law-scholars-conference/program/

———, "The 'Internet of Bodies' Is Here. Are Courts and Regulators Ready?" *Wall Street Journal*, November 12, 2018. As of April 28, 2020: https://www.wsj.com/articles/the-internet-of-bodies-is-here-are-courts-and-regulators-ready-1542039566

———, "The Internet of Bodies," *William & Mary Law Review*, Vol. 77, No. 1, 2019. As of April 28, 2020: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3452891

MDIC—*See* Medical Device Innovation Consortium.

Medical Device Innovation Consortium, *Medical Device Cybersecurity Report: Advancing Coordinated Vulnerability Disclosure*, Minneapolis, Minn., October 1, 2018. As of July 3, 2019: http://mdic.org/wp-content/uploads/2018/10/MDIC-CybersecurityReport.pdf

Meingast, Marci, Tanya Roosta, and Shankar Sastry, "Security and Privacy Issues with Health Care Information Technology," *Proceedings of the 2006 International Conference of the IEEE Engineering in Medicine and Biology Society*, New York, August 31–September 3, 2006, pp. 5453–5458.

Morris, David, "Exercise App Reaches $1 Million FTC Settlement After Breaking Its Promise to Pay Users for Working Out," *Fortune*, September 23, 2017. As of April 28, 2020: https://fortune.com/2017/09/23/exercise-app-pact-settlement/

Moss, Sebastian, "US Sanctions Chinese Tech Companies Including Sensetime over Human Rights Abuses," *Data Center Dynamics*, October 8, 2019. As of April 28, 2020: https://www.datacenterdynamics.com/news/us-sanctions-chinese-tech-companies-including-sensetime-over-human-rights-abuses/

Mulligan, Stephen P., Wilson C. Freeman, and Chris D. Linebaugh, *Data Protection Law: An Overview*, Washington, D.C.: Congressional Research Service, R45631, March 25, 2019. As of April 28, 2020: https://crsreports.congress.gov/product/pdf/R/R45631

National Association of Attorneys General, "Federal Trade Commission Hearings on Competition and Consumer Protection in the 21st Century: Public Comments of 43 State Attorneys General," June 11, 2019. As of April 20, 2020: https://www.washingtonpost.com/context/state-ags-call-for-data-regulations/52f85d7a-c512-4eec-bc50-2ac411e2c593/

National Center for Health Statistics, "Health, United States, 2015: With Special Feature on Racial and Ethnic Health Disparities," 2016.

National Institute of Standards and Technology, "NIST Releases Draft Security Feature Recommendations for IoT Devices," press release, August 1, 2019. As of July 7, 2020: https://www.nist.gov/news-events/news/2019/08/nist-releases-draft-security-feature-recommendations-iot-devices

National Institute of Standards and Technology Cyber Physical Systems Public Working Group, "Framework for Cyber-Physical Systems, Release 1.0," May 2016. As of April 28, 2020: https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf

Neal, Meghan, "The Internet of Bodies Is Coming, and You Could Get Hacked," *Motherboard*, March 13, 2014. As of July 3, 2019: https://www.vice.com/en_us/article/gvyqgm/the-internet-of-bodies-is-coming-and-you-could-get-hacked

Networking and Information Technology Research and Development, "Cyber-Physical System Interagency Working Group (2015) CPS Vision Statement," June 3, 2015. As of November 7, 2019: https://www.nitrd.gov/nitrdgroups/images/6/6a/Cyber_Physical_Systems_(CPS)_Vision_Statement.pdf

Newhouse, William, Stephanie Keith, Benjamin Scribner, and Greg Witte, "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," NIST Special Publication 800-181, August 2017. As of April 28, 2020: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

Ng, Alfred, "Security Flaw Allows for Spying over 5G, Researchers Warn," CNET, February 1, 2019. As of April 28, 2020: https://www.cnet.com/news/security-flaw-allows-for-spying-over-5g-researchers-find/

NIST—*See* National Institute of Standards and Technology.

NITRD—*See* Networking and Information Technology Research and Development.

Oberhaus, Daniel, "This DIY Implant Lets You Stream Movies from Inside Your Leg," *Wired*, August 30, 2019. As of August 30, 2019: https://www.wired.com/story/this-diy-implant-lets-you-stream-movies-from-inside-your-leg/

Office of the National Coordinator for Health Information Technology, "What Is an Electronic Health Record (EHR)?" webpage, HealthIT.gov, September 10, 2019. As of April 28, 2020: https://www.healthit.gov/faq/what-electronic-health-record-ehr

"Official IEEE 802.11 Working Group Project Timelines," Institute of Electrical and Electronics Engineers, September 25, 2019. As of April 28, 2020: http://www.ieee802.org/11/Reports/802.11_Timelines.htm

Okun, Michael S., "Tips for Choosing a Deep Brain Stimulation Device," *JAMA Neurology*, Vol. 76, No. 7, April 2019, pp. 749–750.

Osoba, Osonde A., and William Welser IV, *An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence*, Santa Monica, Calif.: RAND Corporation, RR-1744-RC, 2017. As of April 28, 2020: https://www.rand.org/pubs/research_reports/RR1744.html

Papola, Davide, Chiara Gastaldon, and Giovanni Ostuzzi, "Can a Digital Medicine System Improve Adherence to Antipsychotic Treatment?" *Epidemiology and Psychiatric Sciences*, Vol. 27, No. 3, 2018, pp. 227–229.

Piwek, Lukasz, David A. Ellis, Sally Andrews, and Adam Joinson, "The Rise of Consumer Health Wearables: Promises and Barriers," *PLoS Medicine*, Vol. 13, No. 2, 2016, p. e1001953.

Plowman, R. Scooter, Timothy Peters-Strickland, and George M. Savage, "Digital Medicines: Clinical Review on the Safety of Tablets with Sensors," *Expert Opinion on Drug Safety*, Vol. 17, No. 9, 2018, pp. 849–852.

Purcell, David, H. Irene Hall, Kyle L. Bernstein, Thomas L. Gift, Eugene McCray, and Jonathan Mermin, "The Importance of Population Denominators for High-Impact Public Health for Marginalized Populations," *JMIR Public Health and Surveillance*, Vol. 2, No. 1, May 17, 2016, p. e26.

Ratnam, Gopal, "Progress on Federal Data Privacy Bill Slows in Both Chambers," *Chicago Tribune*, June 26, 2019. As of July 8, 2019: https://www.chicagotribune.com/sns-tns-bc-congress-data-privacy-20190626-story.html

Revised Code of Washington, Chapter 19.375, Biometric Identifiers. As of July 3, 2019: https://app.leg.wa.gov/RCW/default.aspx?cite=19.375

Ross, Julianne, "Smart Scales Measure a Lot More Than Weight," CNN, January 4, 2019. As of April 28, 2020: https://www.cnn.com/2019/01/04/cnn-underscored/best-smart-scales/index.html

Rupert, Douglas J., Rebecca R. Moultrie, Jennifer Gard Read, Jacqueline B. Amoozegar, Alexandra S. Bornkessel, Amie C. O'Donoghue, and Helen W. Sullivan, "Perceived Healthcare Provider Reactions to Patient and Caregiver Use of Online Health Communities," *Patient Education and Counseling*, Vol. 96, No. 3, 2014, pp. 320–326.

Russo, Massimo, and Michael Albert, "How IoT Data Ecosystems Will Transform B2B Competition," *Boston Consulting Group*, July 27, 2018. As of July 3, 2019: https://www.bcg.com/en-us/publications/2018/how-internet-of-things-iot-data-ecosystems-transform-b2b-competition.aspx

Samuel, Sigal, "How Biohackers Are Trying to Upgrade Their Brains, Their Bodies—and Human Nature," *Vox*, June 25, 2019. As of April 28, 2020: https://www.vox.com/future-perfect/2019/6/25/18682583/biohacking-transhumanism-human-augmentation-genetic-engineering-crispr

Savage, Maddy, "Thousands of Swedes Are Inserting Microchips Under Their Skin," NPR, October 22, 2018. As of April 28, 2020: https://www.npr.org/2018/10/22/658808705/thousands-of-swedes-are-inserting-microchips-under-their-skin

Schneeweiss, Sebastian, and Jerry Avorn, "A Review of Uses of Health Care Utilization Databases for Epidemiologic Research on Therapeutics," *Journal of Clinical Epidemiology*, Vol. 58, No. 4, 2005, pp. 323–337.

Schulte, Fred, and Erika Fry, "Death by 1,000 Clicks: Where Electronic Health Records Went Wrong," *Kaiser Health News*, March 18, 2019a. As of April 28, 2020: https://khn.org/news/death-by-a-thousand-clicks/

———, "FDA Chief Calls for Stricter Scrutiny of Electronic Health Records," *Kaiser Health News*, March 21, 2019b. As of April 28, 2020: https://khn.org/news/fda-chief-calls-for-stricter-scrutiny-of-electronic-health-records/

Scott, Emily, "Wearable Device Can Predict Older Adults' Risk of Falling," Carl R. Woese Institute For Genomic Biology, University of Illinois, July 12, 2018. As of April 28, 2020: https://www.igb.illinois.edu/article/wearable-device-can-predict-older-adults-risk-falling

"Security Breach Notification Laws," database, National Conference of State Legislatures, Washington, D.C., updated September 29, 2018. As of April 28, 2020: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Silver, Mike, "Scientists Develop Tiny Tooth-Mounted Sensors That Can Track What You Eat," *Tufts Now*, March 22, 2018. As of July 9, 2019: https://now.tufts.edu/news-releases/scientists-develop-tiny-tooth-mounted-sensors-can-track-what-you-eat

Simons, Joseph, Office of the Chairman, Federal Trade Commission, "Joseph Simons to the Honorable Frank Pallone, Jr., Washington, D.C.," letter, April 1, 2019. As of April 28, 2020: https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/FTC%20Response%20to%20Pallone-Schakowsky.pdf

Slager, Heidi K., Jamie Jensen, Kristin Kozlowski, Holly Teagle, Lisa R. Park, Allison Bieve, and Megan Mears, "Remote Programming of Cochlear Implants," *Otology & Neurotology*, Vol. 40, No. 3, 2019, p. e260.

Smith, Robert Ellis, "Compilation of State and Federal Privacy Laws 2013 Electronic Edition," webpage, *Privacy Journal*, 2013.

Solon, Olivia, "Amazon Patents Wristband That Tracks Warehouse Workers' Movements," *The Guardian*, January 13, 2018. As of April 28, 2020: https://www.theguardian.com/technology/2018/jan/31/amazon-warehouse-wristband-tracking

Stachel, Joshua R., Ervin Sejdić, Ajay Ogirala, and Marlin Mickle, "The Impact of the Internet of Things on Implanted Medical Devices Including Pacemakers, and ICDs," *2013 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*, Minneapolis, Minn., May 6–9, 2013. As of April 28, 2020: https://ieeexplore.ieee.org/document/6555533

Staedter, Tracy, "Satellite Internet Technology Has Ignited a New Space Race," *Now.*, Northrup Grumman, July 3, 2019. As of April 28, 2020: https://now.northropgrumman.com/satellite-internet-technology-has-ignited-a-new-space-race

Steele, Robert, and Andrew Clarke, "The Internet of Things and Next-Generation Public Health Information Systems," *Communications and Network*, Vol. 5, No. 03, 2013, pp. 4–9.

Strathspey Crown, "Strathspey Crown LLC Announces Issuance of US Patent of the First Implantable Intraocular Lens (IOL) with a Video Camera and Wireless Transmission Capability," July 12, 2017. As of April 28, 2020: http://strathspeycrown.com/assets/pdf/1505148854250fc4abc8da4e88d59bf6d0486bf1cc.pdf

Stück, David, Haraldur Tómas, Greg Ver Steeg, Alessandro Epasto, and Luca Foschini, "Novel Digital Voice Biomarkers of Dementia from the Framingham Study," *Alzheimer's & Dementia: The Journal of the Alzheimer's Association*, Vol. 14, No. 7, 2018, pp. 778–779.

Sullivan, Tom, "Why EHR Data Interoperability Is Such a Mess in 3 Charts," *Healthcare IT News*, May 16, 2018. As of April 28, 2020: https://www.healthcareitnews.com/news/why-ehr-data-interoperability-such-mess-3-charts

Swearingen, Jake, "Europe's 'Right to Be Forgotten' Will Be Staying in Europe," *New York Magazine*, January 10, 2019. As of April 28, 2020: http://nymag.com/intelligencer/2019/01/europes-right-to-be-forgotten-will-be-staying-in-europe.html

Texas Business and Commerce Code, Title 11, Subtitle A, Chapter 503, Biometric Identifiers. As of April 28, 2020: https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm

"The Case Against a Right to Be Forgotten," *Law Times*, September 17, 2018. As of April 28, 2020: https://www.lawtimesnews.com/article/the-case-against-a-right-to-be-forgotten-16216/

The Internet of Bodies, "Chat re: IoB–FTC Comm. @ TerrellMcSweeny & @amatwyshyn," Twitter moment, March 7, 2018. As of April 28, 2020: https://twitter.com/i/moments/1062106824449634304

ThreatConnect Research Team, "The Anthem Hack: All Roads Lead to China," *ThreatConnect* blog, February 27, 2015. As of April 28, 2020: https://threatconnect.com/blog/the-anthem-hack-all-roads-lead-to-china/

Tibken, Shara, and Robert Cheng, "Hearing Aids Are Getting Smarter. Think AI, Health Tracking," CNET, April 5, 2018. As of July 9, 2019: https://www.cnet.com/news/hearing-aids-now-theyre-internet-ai-and-health-devices-starkey-oticon-harman-bose/

Trammell, Dustin D., "Differences: Bodyhacking vs Biohacking," in *BodyHackingCon* blog, September 26, 2015. As of April 28, 2020: https://bodyhackingcon.com/blog/differences-bodyhacking-vs-biohacking.html

Trauth, Erin, and Ella Browning, "Technologized Talk: Wearable Technologies, Patient Agency, and Medical Communication in Healthcare Settings," *International Journal of Sociotechnology and Knowledge Development (IJSKD)*, Vol. 10, No. 3, 2018, pp. 1–26.

Turk, Victoria, "This Sleep-Tracking Ring Can Detect When You've Drunk Too Much," *Wired*, June 18, 2019. As of April 28, 2020: https://www.wired.co.uk/article/oura-ring-uk-sleep-tracking

United Nations, *World Population Ageing 2015 (ST/ESA/SER.A/390)*, New York: United Nations Department of Economic and Social Affairs Population Division, 2015.

University of Southern California Center for Body Computing, "Cybersecurity in Healthcare: How California Business can Lead," white paper, 2018. As of April 28, 2020: https://www.uscbodycomputing.org/uncensored/2018/9/24/z6l7c4u7dmu6dqi1e5rvmc7hhujlh6

U.S. Code, Title 15, Section 45, Unfair Methods of Competition Unlawful; Prevention by Commission.

U.S. Consumer Product Safety Commission, "Provata Health Recalls Promotional Activity Trackers Due to Burn Hazard," September 25, 2018. As of April 27, 2020: https://www.cpsc.gov/Recalls/2018/Provata-Health-Recalls-Promotional-Activity-Trackers-Due-to-Burn-Hazard

U.S. Department of Health and Human Services, "Health Information of Deceased Individuals: 45 CFR 160.103, Paragraph (2)(iv) of the Definition of 'Protected Health Information,'" September 2013. As of April 28, 2020: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/health-information-of-deceased-individuals/index.html

U.S. Food and Drug Administration, "Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software," January 14, 2005. As of July 3, 2019: https://www.fda.gov/media/72154/download

———, "Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff," December 28, 2016. As of April 28, 2020: https://www.fda.gov/media/95862/download

———, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff," October 18, 2018d. As of July 3, 2019: https://www.fda.gov/media/86174/download

———, "FDA Approves First Continuous Glucose Monitoring System with a Fully Implantable Glucose Sensor and Compatible Mobile App for Adults with Diabetes," press release, June 25, 2018b. As of April 28, 2020: https://www.fda.gov/news-events/press-announcements/fda-approves-first-continuous-glucose-monitoring-system-fully-implantable-glucose-sensor-and

———, "Medical Device Overview," webpage, September 14, 2018a. As of April 28, 2020: https://www.fda.gov/industry/regulated-products/medical-device-overview

———, "Medical Device Recalls," webpage, September 26, 2018c. As of April 28, 2020: https://www.fda.gov/medical-devices/medical-device-safety/medical-device-recalls

———, "Cybersecurity," webpage, June 27, 2019a. As of July 3, 2019: https://www.fda.gov/medical-devices/digital-health/cybersecurity

———, "Cybersecurity Vulnerabilities Affecting Medtronic Implantable Cardiac Devices, Programmers, and Home Monitors: FDA Safety Communication," webpage, March 21, 2019b. As of April 28, 2020: https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-affecting-medtronic-implantable-cardiac-devices-programmers-and-home

———, "Public Workshop—Content of Premarket Submissions for Management of Cybersecurity in Medical Devices January 29–30, 2019," webpage, January 2019c. As of April 28, 2020: https://www.fda.gov/medical-devices/workshops-conferences-medical-devices/public-workshop-content-premarket-submissions-management-cybersecurity-medical-devices-january-29-30

U.S. Immigration and Customs Enforcement (ICE), "Law Enforcement Information Sharing Initiative," webpage, U.S. Department of Homeland Security, undated. As of April 28, 2020: https://www.ice.gov/le-information-sharing

Vaas, Lisa, "Doctors Disabled Wireless in Dick Cheney's Pacemaker to Thwart Hacking," *Naked Security*, October 22, 2013. As of April 28, 2020: https://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/

Verheij, Robert A., Vasa Curcin, Brendan C. Delaney, and Mark M. McGilchrist, "Possible Sources of Bias in Primary Care Electronic Health Record Data Use and Reuse," *Journal of Medical Internet Research*, Vol. 20, No. 5, 2018, p. e185.

Vermont Public Law H.764 (Act 171), An Act Relating to Data Brokers and Consumer Protection, May 22, 2018. As of April 28, 2020: https://legislature.vermont.gov/bill/status/2018/H.764

Vita-More, Natasha, "Life Extension Leadership Meetings, Conferences, and Festivals," *H Plus Magazine*, July 22, 2018.

Wang, Echo, "China's Kunlun Tech Agrees to U.S. Demand to Sell Grindr Gay Dating App," Reuters, May 13, 2019. As of April 28, 2020: https://www.reuters.com/article/us-grindr-m-a-beijingkunlun/chinas-kunlun-tech-agrees-to-u-s-demand-to-sell-grindr-gay-dating-app-idUSKCN1SJ28N

Waters, Michael, "The Smart Diaper Is Coming. Who Actually Wants It?" *Vox*, May 2, 2019. As of April 28, 2020: https://www.vox.com/the-goods/2019/5/2/18525487/smart-diaper-huggies-monit-pampers-alert-poop-pee

Wee, Sui-Lee, "China Uses DNA to Track Its People, with the Help of American Expertise," *New York Times*, February 21, 2019. As of July 3, 2019: https://www.nytimes.com/2019/02/21/business/china-xinjiang-uighur-dna-thermo-fisher.html

Whittaker, Zack, "Justice Department Charges Chinese Hacker for 2015 Anthem Breach," *TechCrunch*, May 9, 2019. As of April 28, 2020: https://techcrunch.com/2019/05/09/anthem-breach-indictment

Wicklund, Eric, "FDA Approves mHealth Wearable for Tracking Epileptic Seizures," *mHealth Intelligence*, February 6, 2018. As of April 29, 2020: https://mhealthintelligence.com/news/fda-approves-mhealth-wearable-for-tracking-epileptic-seizures

Wisconsin Statutes §134.98, Notice of Unauthorized Acquisition of Personal Information. As of April 29, 2020: https://docs.legis.wisconsin.gov/statutes/statutes/134/98

Woods, Beau, Andrea Coravos, and Joshua David Corman, "The Case for a Hippocratic Oath for Connected Medical Devices: Viewpoint," *Journal of Medical Internet Research*, Vol. 21, No. 3, 2019. As of July 3, 2019: https://www.jmir.org/2019/3/e12568/pdf

Wootson, Cleve R., "A Man Detailed His Escape from a Burning House. His Pacemaker Told Police a Different Story," *Washington Post*, February 8, 2017. As of July 3, 2019: https://www.washingtonpost.com/news/to-your-health/wp/2017/02/08/a-man-detailed-his-escape-from-a-burning-house-his-pacemaker-told-police-a-different-story/?utm_term=.f0b9a4d2b9dd

World Health Organization, "Noncommunicable Diseases," fact sheet, June 1, 2018. As of April 28, 2020: https://www.who.int/news-room/fact-sheets/detail/noncommunicable-diseases

Yang, Tingting, Dan Xie, Zhihong Li, and Hongwei Zhu, "Recent Advances in Wearable Tactile Sensors: Materials, Sensing Mechanisms, and Device Performance," *Materials Science and Engineering: R: Reports*, Vol. 115, 2017, pp. 1–37.

Yu, Kun-Hsing, and Isaac S. Kohane, "Framing the Challenges of Artificial Intelligence in Medicine," *BMJ Quality & Safety*, Vol. 28, 2019, pp. 238–241.

Zaino, Jennifer, "5G vs. 4G Cellular Technology: What Businesses Need to Know," *BizTech*, August 6, 2019. As of April 29, 2020: https://biztechmagazine.com/article/2019/09/5g-vs-4g-cellular-technology-what-businesses-need-know-perfcon

Zhang, Sarah, "People Are Clamoring to Buy Old Insulin Pumps," *The Atlantic*, April 29, 2019. As of July 7, 2020: https://www.theatlantic.com/science/archive/2019/04/looping-created-insulin-pump-underground-market/588091/

Zlotolow, Dan A., and Scott H. Kozin, "Advances in Upper Extremity Prosthetics," *Hand Clinics*, Vol. 28, No. 4, 2012, pp. 587–593.

Zraick, Karen, and Sarah Mervosh, "That Sleep Tracker Could Make Your Insomnia Worse," *New York Times*, June 13, 2019. As of April 29, 2020: https://www.nytimes.com/2019/06/13/health/sleep-tracker-insomnia-orthosomnia.html?module=inline

Acknowledgments

The authors are deeply indebted to Jacques Dubois for his generous donation to RAND's Center for Global Risk and Security (CGRS), which made this work possible. The authors also thank the CGRS Advisory Board, as well as Robin Meili, King Mallory, and Casey Bouskill, for making this project possible.

We would like to thank Caolionn O'Connell for advising the team and Sonni Efron for her skillful editorial assistance. We would also like to thank our reviewers, Marjory Blumenthal, senior policy researcher at the RAND Corporation, and Patricia Stapleton, comparative political science and public policy scholar at RAND, for their thoughtful comments on this report, and Rick Penn-Kraus for his illustrations.

We would also like to thank the following people for valuable discussions and insights: Penny Chase, James Christensen, Steven Christey, Al Emondi, Angel Giuffria, Amal Graafstra, Matthew Hepburn, Timothy Hanson, Robert Klitzman, and Beau Woods.

Any errors in this article are the authors' own.

About the Authors

Mary Lee is a mathematician at the RAND Corporation and inaugural Fellow for RAND's Center for Global Risk and Security. Her research interests include mathematical modeling and simulation of complex systems in the areas of defense/aerospace, cyber policy, and health care and chronic diseases.

Benjamin Boudreaux is a professor at Pardee RAND Graduate School and a policy researcher at RAND working in the intersection of national security, technology, and ethics. His current research focuses on ethical issues in artificial intelligence, social media policy, and cyber incident response.

Ritika Chaturvedi was an engineer at the RAND Corporation during this project. She is currently serving as a research scientist at the Schaeffer Center for Health Policy and Economics at the University of Southern California. She has a diverse background in engineering, science and technology policy, asset valuation, strategic consulting, and translational biomedical research. She is interested in science and technology questions regarding the broad effects of emerging disruptive technologies in the life sciences and health care and on society.

Sasha Romanosky is a policy researcher at the RAND Corporation and former cyber policy advisor to the Pentagon in the Office of the Secretary of Defense for Policy. He researches topics in the economics of security and privacy, national security, applied microeconomics, and law and economics.

Bryce Downing is a research assistant at the RAND Corporation. Before joining RAND, he was a strategic simulations intern at the U.S. Army War College, Center for Strategic Leadership. His research interests include technology policy, modeling decisionmaking under uncertainty, and national security.

About This Report

The work described in this report was conducted as part of a fellowship awarded by the RAND Corporation's Center for Global Risk and Security. This report describes emerging technologies, herein referred to as the *Internet of Bodies*; analyzes their benefits and risks; and suggests ways various stakeholders can balance those benefits and risks. This report should be of interest to the general public, Internet of Bodies and medical device makers, health-care providers, and policy decisionmakers. The research was conducted within the Center for Global Risk and Security between February 2019 and September 2019.

Funding

Funding for this report was provided by a generous grant from Jacques Dubois.

About the RAND Center for Global Risk and Security

The Center for Global Risk and Security works across the RAND Corporation to develop multidisciplinary research and policy analysis dealing with systemic risks to global security. The center draws on RAND's expertise to complement and expand RAND research in many fields, including security, economics, health, and technology. A board of distinguished business leaders, philanthropists, and former policymakers advises and supports the center's activities, which are increasingly focused on global security trends and the impact of disruptive technologies on risk and security. For more information about the RAND Center for Global Risk and Security, visit www.rand.org/international/cgrs.

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. RAND® is a registered trademark.

Limited Print and Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited. Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please visit www.rand.org/pubs/permissions.

For more information on this publication, visit www.rand.org/t/RR3226.

© 2020 RAND Corporation

www.rand.org

Internet-connected “smart” devices are increasingly available in the marketplace, promising consumers and businesses improved convenience and efficiency. Within this broader Internet of Things (IoT) lies a growing industry of devices that monitor the human body and transmit the data collected via the internet. This development, which some have called the Internet of Bodies (IoB), includes an expanding array of devices that combine software, hardware, and communication capabilities to track personal health data, provide vital medical treatment, or enhance bodily comfort, function, health, or well-being. However, these devices also complicate a field already fraught with legal, regulatory, and ethical risks. The authors of this report examine this emerging collection of human body–centric and internet-connected technologies; explore benefits, security and privacy risks, and ethical implications; survey the nascent regulatory landscape for these devices and the data they collect; and make recommendations to balance IoB risks and rewards.

$19.00

ISBN-10 1-9774-0522-3
ISBN-13 978-1-9774-0522-7

51900

9 781977 405227

www.rand.org

RR-3226-RC

View publication stats